SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 19/2807**
19. Wahlperiode 23. März 2021

Bericht

des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

Tätigkeitsbericht 2021

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

TÄTIGKEITSBERICHT
2021

Tätigkeitsbericht 2021
des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

BERICHTSZEITRAUM: 2020

REDAKTIONSSCHLUSS: 31.12.2020

LANDTAGSDRUCKSACHE 19/2807

(39. TÄTIGKEITSBERICHT DER LANDESBEAUFTRAGTEN FÜR DATENSCHUTZ)

Marit Hansen

Landesbeauftragte für Datenschutz Schleswig-Holstein

Leiterin des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Mail: mail@datenschutzzentrum.de

Web: https://www.datenschutzzentrum.de

Satz und Lektorat: Gunna Westphal, Kiel

Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel

Titelfoto: ULD, Kiel

Druck: hansadruck und Verlags-GmbH & Co KG, Kiel

Inhaltsverzeichnis

01

KERNPUNKTE

Jahresthema: Corona

Zahlen und Fakten

Digitalisierung in Schleswig-Holstein

1 Datenschutz und Informationsfreiheit

In unserem Tätigkeitsbericht haben mein Team und ich die wichtigsten und interessantesten Themen und Fälle im Jahr 2020 aus den Bereichen Datenschutz und Informationsfreiheit zusammengestellt, um Ihnen einen Eindruck unserer Arbeit und Erfolge zu vermitteln. Dieses Jahr stand stark unter dem Eindruck der Coronapandemie: Die Bedrohungen durch das Virus SARS-CoV-2 haben große Unsicherheiten für die Bevölkerung, Firmen und Behörden mit sich gebracht. Immer wieder musste die Lage neu eingeschätzt werden. Dies betrifft auch den Umgang mit Grundrechten wie dem Datenschutz. Dieses Thema mit vielfältigen Facetten durchzieht daher den vorliegenden Bericht: Wie sieht Datenschutzkonformität bei der Verarbeitung personenbezogener Daten in der Pandemiesituation aus?

Zum Bericht gehören selbstverständlich auch die Prüfungen, die meine Dienststelle, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) durchgeführt hat – wobei fast überall erhebliche Mängel sichtbar wurden. Die meisten Verantwortlichen haben schnell reagiert, um die Mängel abzustellen.

In dem Berichtsjahr stand auch die Wahl der oder des Landesbeauftragten für Datenschutz auf der Tagesordnung der Parlamentarier. Ich wurde in der Landtagssitzung vom 18.06.2020 für meine zweite Amtszeit wiedergewählt. Ministerpräsident Daniel Günther hat mir die Ernennungsurkunde am 28.09.2020 überreicht. Das war zugleich der erste Tag meiner zweiten sechsjährigen Amtszeit.

Eines ist jetzt schon klar – und das zeigt sich schon beim Durchblättern unseres Tätigkeitsberichts: Die interessanten Themen werden in den nächsten sechs Jahren nicht ausgehen. Es gilt, die fortschreitende Digitalisierung im Sinne der Grundrechte und Menschenrechte zu gestalten. Für die Themen Datenschutz und Informationsfreiheit werden wir uns dabei weiterhin im Rahmen unserer Aufgaben und Zuständigkeiten einbringen.

Ich wünsche Ihnen eine interessante Lektüre unseres Tätigkeitsberichts!

Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein

1.1 Jahresthema: Corona

Es erstaunt wohl niemanden, dass die Arbeit einer Datenschutzbehörde stark von den **Auswirkungen der Coronapandemie** geprägt wird.

Welche Eingriffe sind verhältnismäßig, welche nicht? Gibt es mildere Mittel, um das Ziel der Pandemiebekämpfung zu erreichen? Braucht man neue Datenbanken im Gesundheitswesen? Wie funktioniert ein sicherer Austausch der Daten, wie werden Zugriffsberechtigungen nachgewiesen? Welche Techniken, die Homeoffice oder Homeschooling unterstützen, sind datenschutzkonform? Muss man wirklich die betrieblichen und behördlichen Datenschutzbeauftragten einbeziehen, wenn man die Prozesse zur Verarbeitung personenbezogener Daten ändert? Wenn – wie bei der Kontaktdatenerfassung – zwangsweise Daten gesammelt werden müssen, darf man diese Daten nicht auch zu anderen wirtschaftlichen Zwecken nutzen? Und warum sollte nicht auch die Polizei auf alle Daten zugreifen können? Basiert die Corona-Warn-App wirklich auf datenschutzfreundlichen Konzepten? Ohne Standortdaten kann das nicht funktionieren, oder? Würden Sie die App nutzen?

Solche Fragen haben wir bald täglich erhalten. Einiges ließ sich schnell beantworten, für andere Sachverhalte waren tiefgründigere Prüfungen nötig. Aber auch hier waren die Mitarbeiterinnen und Mitarbeiter mit besonderem Einsatz und unter Berücksichtigung eiliger Fristen tätig. Umso unverständlicher, dass auch im Jahr 2021 noch in Talkshows kolportiert wird, Datenschutz würde Gesundheitsschutz verhindern. **In jedem konkreten Fall** ließen sich **vermeintliche Konflikte auflösen**, sobald genau die Zwecke, die geplanten Verarbeitungen, die Beteiligten und die Verantwortlichkeiten kommuniziert wurden.

Auf der Ebene der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder haben wir im April 2020 klargestellt, dass **auch in Krisenzeiten die Datenschutzgrundsätze gelten**, und geeignete Garantien zum Schutz

der betroffenen Personen – das ist die ganze Bevölkerung – eingefordert.

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 03.04.2020: **Datenschutzgrundsätze bei der Bewältigung der Coronapandemie:**

https://www.datenschutzkonferenz-online.de/media/en/Entschließung Pandemie 03_04_2020_final.pdf

Kurzlink: *https://uldsh.de/tb39-1-1*

Coronathemen spiegeln sich auch in unserer Tätigkeit und in diesem Bericht wider:

Coronamaßnahmen in der Verwaltung wie Fragebögen (Tz. 4.1.1) oder Temperaturmessung beim Rathausbesuch (Tz. 4.1.2), Kontaktdatenerfassung in der Justiz (Tz. 4.3.2) und in der Wirtschaft (Tz. 5.3) mit zahlreichen Einzelproblemen (Tz. 5.4.1, Tz. 5.4.2), auch im Vereinsleben (Tz. 5.4.3), Fragen der Zugriffsmöglichkeiten auf Kontaktdaten durch die Polizei (Tz. 4.2.4), WLAN-Nutzung für die Corona-„Strandampel“ (Tz. 7.1), datenschutzkonforme App-Entwicklung (Tz. 8.1) und unsere Aussagen der Datenschutzaufsichtsbehörden in Europa zur Kontaktnachverfolgung (Tz. 11.1).

Hinzu kommen **Digitalisierungsvorhaben**, die eingeführt werden, um einen Ersatz für Präsenztreffen und Anwesenheit vor Ort zu bieten: Ton- und Videoaufnahmen in kommunalen Sitzungen (Tz. 4.1.3), digitaler Schulunterricht (Tz. 4.1.5), Online-Prüfung von Sozialdaten (Tz. 4.4.1), Videokonferenzsysteme (Tz. 6.3.2) sowie die Bedingungen für Homeoffice (Tz. 6.3.3), damit Datenpannen im Lockdown (Tz. 5.5.1) vermieden werden.

Was ist zu tun?

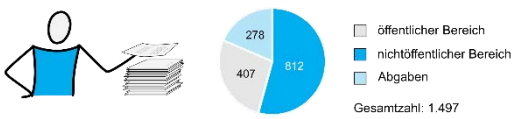
Die Landesbeauftragte für Datenschutz steht mit ihrem Team bereit, um die weiterhin drängenden und sich immer wieder in neuen Situationen stellenden Fragen zu Datenschutz bei Coronamaßnahmen und zur fortschreitenden Digitalisierung zu klären, um Lösungen zu finden, bei denen die Grundrechte der Menschen auch in der Pandemiesituation gewahrt werden.

1.2 Zahlen und Fakten zum Jahr 2020

Die pandemiebedingten Lockdown-Zeiten im Jahr 2020 haben nicht dazu geführt, dass Beschwerden oder Datenpannen ausgeblieben sind. In fast allen Bereichen ist sogar eine Zunahme zu verzeichnen:

2020 erreichten uns 1.497 schriftliche **Beschwerden** (Vorjahr: 1.194), von denen 278 (Vorjahr: 235) nicht in unserer Zuständigkeit (öffentliche und nichtöffentliche Stellen in Schleswig-Holstein mit Ausnahme bestimmter Bereiche in Bundeszuständigkeit, z. B. Telekommunikation) lagen und an die zuständigen Behörden abgegeben werden mussten.

Da bei uns erhobene Beschwerden zunehmend einen **grenzüberschreitenden Sachverhalt** oder Verantwortliche in anderen Mitgliedstaaten betreffen, werden regelmäßig Fälle an die zuständigen Aufsichtsbehörden anderer Mitgliedstaaten zur alleinigen oder federführenden Bearbeitung abgegeben. Im Jahr 2020 betraf dies u. a. die Aufsichtsbehörden in Dänemark, Frankreich, Irland, Italien, Schweden und dem Vereinigten Königreich (UK).



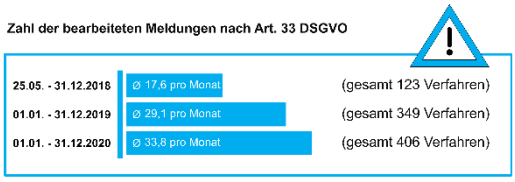
Zahl der bearbeiteten Beschwerden im Jahr 2020

Insgesamt wurden in eigener Zuständigkeit 1.219 (Vorjahr: 959) Beschwerden bearbeitet, davon richteten sich mehr als zwei Drittel der Beschwerden gegen Unternehmen und andere nichtöffentliche Stellen (812; Vorjahr: 680), der Rest gegen Behörden (407; Vorjahr: 279). Dazu kamen 808 (Vorjahr: 758)

Beratungen für den öffentlichen und den nichtöffentlichen Bereich.

Ohne vorherige Beschwerde wurden 8 (Vorjahr: 10) **Prüfungen** im öffentlichen und 5 (Vorjahr: 13) im nichtöffentlichen Bereich begonnen und neue Verfahren eingeleitet; zahlreiche Prüfungen aus dem Vorjahr wurden fortgeführt.

Die Zahl von 406 (Vorjahr: 349) gemeldeten **Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 DSGVO (Datenpannen)** ist zwar schon recht hoch – an jedem Arbeitstag erreichen uns mehrere Meldungen oder nähere Erläuterungen zu schon getätigten Meldungen. Dennoch erfahren wir auch immer wieder von Datenpannen, bei denen die Verantwortlichen der Meldepflicht nicht nachgekommen sind.



Von den **Abhilfemaßnahmen** als Reaktion auf festgestellte Verstöße gegen das Datenschutzrecht wurde im Berichtsjahr insgesamt wie folgt Gebrauch gemacht:

- 42 Warnungen (Vorjahr: 37),
- 50 Verwarnungen (Vorjahr: 26),
- 13 Anordnungen zur Änderung oder Einschränkung der Verarbeitung (Vorjahr: 2).

Eine Geldbuße wurde im Jahr 2020 (wie auch im Jahr 2019) nicht verhängt.

Nach unserem Eindruck wird die Dienststelle der Landesbeauftragten für Datenschutz in **Gesetzgebungsvorhaben** auf Landesebene schon weitgehend eingebunden, wenn Aspekte des Datenschutzes oder des Informationszugangs betroffen sein könnten. Dies geschah im Berichtsjahr über die Arbeitsebene parallel zur Anhörung von Verbänden oder über die Ausschüsse im Landtag in 25 (Vorjahr: 39) neuen Gesetzgebungsvorhaben; ein Teil der Vorjahresbeteiligungen erstreckte sich zudem auf das Jahr 2020.

1.3 Digitalisierung in Schleswig-Holstein

Schleswig-Holstein hat Digitalisierung als ein wichtiges Thema erkannt – nicht erst seit der Coronapandemie: Im Jahr 2020 wurden aus der Notwendigkeit, die persönlichen Treffen zu reduzieren und das Arbeiten zumindest teilweise ins Homeoffice zu verlagern, digitale Möglichkeiten zur Kommunikation und Kooperation stark nachgefragt. Dies betraf zahlreiche Bereiche, beispielsweise Bildung, Gesundheit, Politik, Verwaltung und Wirtschaft.

Kollisionen der kurzfristig zu erfüllenden Bedarfe mit den längerfristigen Planungen, die seit Jahren verfolgt werden, waren nicht zu vermeiden. Auch mussten Prioritäten verändert werden. Ein Beispiel ist die grundsätzliche Beschäftigung mit dem Thema der künstlichen Intelligenz (KI): In dem **Beirat „KI@Gesellschaft“** diskutieren seit Juni 2020 elf von der Staatskanzlei eingeladene Expertinnen und Experten, darunter auch die Landesbeauftragte für Datenschutz, notwendige Änderungen des Rechtsrahmens und ethische Leitlinien für die Anwendung von KI. Dort sollen „ein Zielbild für den gesellschaftsdienlichen, unschädlichen Einsatz von KI“ und „Positionspapiere für den Einsatz von künstlicher Intelligenz in bestimmten Anwendungsfällen, beispielsweise in der Medizin“ erarbeitet werden.

Die ehrgeizige Zeitplanung sah mehrere Sitzungen und schnelle Ergebnisse vor, doch die Treffen konnten großenteils nicht wie geplant stattfinden. Immerhin konnten sich Bürgerinnen und Bürger anlässlich der öffentlichen Sitzung des Expertenrats auf der „Digitalen Woche Kiel“ im September einen ersten Eindruck über die vielfältigen Themen verschaffen, mit denen sich der Beirat beschäftigt. Die Arbeiten werden im Jahr 2021 fortgesetzt.

https://www.schleswig-holstein.de/DE/Landesregierung/Themen/Digitalisierung/Digitalisierung/KI_Strategie/_documents/gesellschaft.html

Kurzlink: *https://uldsh.de/tb39-1-3*

Von besonderer Bedeutung und mit Strahlkraft über die Landesgrenzen hinaus ist außerdem die **Open-Source-Strategie des Landes** (37. TB,

Tz. 1.3), die sich über die letzten Jahre weiterentwickelt hat. Wir begrüßen die Initiative der Landesregierung zur Umstellung auf Open Source, auch und gerade im Sinne einer digitalen Souveränität (Tz. 2.1) und zum Nutzen des Datenschutzes.

Was ist zu tun?

Schleswig-Holstein kann positive Impulse für eine Digitalisierung setzen, die gut für Mensch und Gesellschaft ist. Gern unterstützen wir dabei.

1.4 Fortschreiben der gesetzlichen Regelungen zu Datenschutz und Informationsfreiheit

Bei der Anwendung von Gesetzen kann man viel lernen – insbesondere wenn es in der Praxis hakt oder in Einzelfällen die Intention des Gesetzgebers ins Gegenteil verkehrt scheint, weil Formulierungen missverständlich gewählt wurden. Wird man dieser Probleme gewahr, sollte der Gesetzgeber nachbessern. Um dies nicht dem Zufall zu überlassen, sehen zahlreiche Gesetze mittlerweile Evaluationsklauseln vor, darunter auch die Datenschutz-Grundverordnung, das Bundesdatenschutzgesetz und das Landesdatenschutzgesetz Schleswig-Holstein.

Den Auftakt machte die **Evaluation der DSGVO**. Der Evaluationsbericht war eigentlich schon im Mai erwartet worden (38. TB, Tz. 2.4), doch dies verschob sich auf Juni 2020. Im Ergebnis bestätigt der Bericht, dass die DSGVO zurzeit unverändert bleiben soll. Allerdings wurde in der Evaluation festgestellt, dass noch nicht das volle Potenzial der DSGVO ausgeschöpft wird. Der Bericht fordert insbesondere, dass die vorgesehenen Instrumente in vollem Umfang genutzt werden sollen. Betrachtet wurde auch die Umsetzung der DSGVO in den Mitgliedstaaten, wo Baustellen erkannt wurden, wenn die Staaten europäische Regelungen gar nicht oder fehlerhaft umgesetzt haben. Im Evaluierungsbericht wird gefordert, „**ein harmonisiertes Konzept und eine gemeinsame europäische Datenschutzkultur**“ zu schaffen und **„eine effizientere und einheitlichere Bearbeitung grenzüberschreitender Fälle“** zu fördern.

In diesem Sinne werden den Mitgliedstaaten, dem Europäischen Datenschutzausschuss und den Datenschutzbehörden sowie der Kommission selbst zahlreiche Aufgaben ins Stammbuch geschrieben, die im nächsten Evaluationsbericht im Jahr 2024 besondere Beachtung finden werden.

EU-Kommission: **Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung:**

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0264

Kurzlink: *https://uldsh.de/tb39-1-4*

Auch für das **BDSG** steht eine Evaluierung an, an der wir uns aufgrund unserer Erfahrungen in der Anwendung ab Ende 2020 beteiligen.

Im **LDSG** Schleswig-Holstein findet sich ebenfalls eine Evaluierungsklausel: Erste Besprechungen zu dem Themenkreis haben bereits stattgefunden; im Jahr 2021 werden sicherlich weitere Punkte erörtert werden.

§ 16 IZG-SH

Die Landesregierung überprüft die Auswirkungen dieses Gesetzes mit wissenschaftlicher Unterstützung. Sie legt dem Landtag dazu in den Jahren 2020 und 2025 einen Bericht vor. Die oder der Landesbeauftragte für Datenschutz ist vor der Zuleitung der Berichte an den Landtag zu unterrichten; sie oder er gibt dazu eine Stellungnahme ab.

Änderungen wären aus unserer Sicht im Bereich Informationsfreiheit, nämlich im **Informationszugangsgesetz Schleswig-Holstein** (IZG-SH) sinnvoll oder sogar **erforderlich**. Dies erläutern wir in

dem Kapitel 12 zur Informationsfreiheit (Tz. 12.1 und Tz. 12.6).

Auch hier gibt es übrigens eine Evaluationsklausel, nach der eigentlich ein Bericht für das Jahr 2020 vorgesehen war – hier muss es wohl Verzögerungen gegeben haben. Wir werden in diesem Zusammenhang unsere Erfahrungen einbringen – spätestens in unserer Stellungnahme zu dem Berichtsentwurf, die wir nach § 16 IZG-SH vor der Zuleitung an den Landtag abgeben werden.

Was ist zu tun?

Wird bei der Evaluation der Gesetze ein Änderungsbedarf festgestellt, sollten die nötigen Nachbesserungen zügig umgesetzt werden.

1.5 Grundrechtskonforme Gestaltungsanforderungen auch international sichtbar

Maßgeblich für unsere Tätigkeiten sind die rechtlichen Grundlagen auf EU-, Bundes- und Landesebene. Aber auch international lohnt es sich, Anforderungen an grundrechtskonforme Gestaltung von IT-Systemen zu kommunizieren. Allerdings können wir als Landesbehörde an den internationalen Konferenzen der Datenschutzbeauftragten und der Informationsfreiheitsbeauftragten nur im Ausnahmefall teilnehmen. Durch Zuarbeiten an die jeweiligen deutschen Vertreterinnen und Vertreter von Bund und Ländern gelingt es dennoch immer wieder, unsere Punkte einzubringen – auch wenn es manchmal länger dauert.

Ein Beispiel sind die mit unserer maßgeblichen Beteiligung erarbeiteten Stellungnahmen zu Transparenz bei Algorithmen und in Systemen der künstlichen Intelligenz für den Einsatz im öffentlichen Bereich aus dem Jahr 2018 (37. TB, Tz. 2.2.3; 38. TB, Tz. 1.5). Im April 2019 wurde dann für die **Internationale Konferenz der Informationsfreiheitsbeauftragten** von Deutschland ein Entwurf für eine Resolution eingebracht, die die wesentlichen Forderungen aus dem Positionspapier deutscher Informationsfreiheitsbeauftragter enthält, die „Draft resolution: **Transparency of public administration when using algorithms is indispensable for the protection of fundamental human and civil rights**“:

https://www.informationcommissioners.org/draft-resolution-transparency-of-public-administration-when-using-algorithms-is-indispensable-for-the-protection-of-fundamental-human-and-civil-rights

Kurzlink: *https://uldsh.de/tb39-1-5*

Dieser Entwurf, der bereits Unterstützer gefunden hatte, sollte in der Folgekonferenz im Jahr 2020 diskutiert werden. Leider konnte bedingt durch die Coronapandemie in dem Jahr die Internationale Konferenz der Informationsfreiheitsbeauftragten nicht stattfinden. Damit verschiebt sich die internationale Behandlung des Themas auf das Jahr 2021. Dennoch hat bereits die Veröffentlichung dieses Entwurfs dafür gesorgt, Impulse zur grundrechtskonformen Gestaltung aus Schleswig-Holstein auf der internationalen Ebene sichtbar zu machen.

1.6 Vorschau: Vorsitz der Konferenz der Informationsfreiheitsbeauftragten im Jahr 2022

Alle Landesbeauftragten für Datenschutz sowie der Bundesbeauftragte in Deutschland sind Mitglied der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Ein ähnliches Gremium ist die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder (IFK), in dem sich die Informationsfreiheitsbeauftragten versammeln – in Deutschland wird diese Rolle auf Bundesebene und in denjenigen Ländern, die über ein Informationsfreiheits- oder Transparenzgesetz verfügen, von den jeweiligen Beauftragten für Datenschutz ausgefüllt. Wie man dies auch von anderen Bund-Länder-Gremien kennt, wechselt der Vorsitz jährlich. Oft richtet sich die Reihenfolge nach dem Alphabet der Namen der Bundesländer, doch es kann auch getauscht werden, wenn besondere Umstände es erfordern.

Für Schleswig-Holstein bedeutet die aktuelle Planung, dass wir **im Jahr 2022** die Ehre haben, die **Leitung der IFK** zu übernehmen. Im **Folgejahr** werden wir dann den **Vorsitz der DSK** innehaben. Angesichts der notwendigen und sinnvollen Abstimmungsbedarfe unter den Behörden ist die Leitung dieser Gremien eine wichtige und arbeitsame Rolle. Wir werden berichten.

02

KERNPUNKTE

Digitale Souveränität

Beschäftigtendatenschutz

EuGH-Urteil „Schrems II“

2 Datenschutz – global und national

Es passiert so viel im Datenschutz auf internationaler, europäischer und nationaler Ebene, wovon auch wir als Datenschutzaufsicht und die Schleswig-Holsteinerinnen und Schleswig-Holsteiner betroffen sein können, dass hier gar nicht erst der Versuch gemacht wird, ein vollständiges Bild zu zeichnen. Herausgegriffen werden wichtige Gestaltungsthemen wie die digitale Souveränität (Tz. 2.1), die Verschlüsselung (Tz. 2.2), die Harmonisierungs- und Zentralisierungsdebatte (Tz. 2.3), das Thema Beschäftigtendatenschutz (Tz. 2.4) und das EuGH-Urteil „Schrems II“, mit dem u. a. der Privacy Shield für ungültig erklärt wurde (Tz. 2.5).

2.1 Digitale Souveränität – souverän planen und umsetzen

Im Datenschutzrecht gilt eine einfache Aussage: „Der Verantwortliche ist verantwortlich.“ So simpel dies klingt: Einfach ist es nicht, seiner Verantwortlichkeit im besten Sinne nachkommen zu können, wenn man sich auf den Einsatz von Technik oder Dienstleistern angewiesen fühlt und dabei nicht wirklich kontrollieren kann, ob alles rechtskonform abläuft. In vielen Fällen ist eine faktische Abhängigkeit von marktbeherrschenden Akteuren nicht von der Hand zu weisen.

Zu den Datenschutzanforderungen gehört aber Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten, gegebenenfalls unter Hinzuziehung des jeweiligen Auftragsverarbeiters.

Digitale Souveränität – Definition des Kompetenzzentrums Öffentliche IT

Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

In verschiedenen Zusammenhängen wird hier die digitale Souveränität gefordert. Das ist aus Datenschutzsicht zu unterstützen. Für den Bereich der öffentlichen Verwaltung hat daher die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die notwendigen Elemente für eine digitale Souveränität konkretisiert:

Langfristig sieht die DSK die Notwendigkeit für den Einsatz von Open-Source-Software in der Verwaltung. Bundesländer wie **Schleswig-Holstein**, die bereits einige Schritte auf dem Weg ihrer Open-Source-Strategie gegangen sind, können nach unserer Überzeugung eine **Vorreiterrolle** einnehmen.

Konkret hält die DSK die folgenden Maßnahmen zum Stärken der digitalen Souveränität von Bund, Ländern und Kommunen für notwendig:

- verbesserte Möglichkeiten der **datenschutzrechtlichen Beurteilung** von Produkten und Dienstleistungen – sowohl bei der Auswahl als auch im laufenden Betrieb,
- Berücksichtigung der Ziele und Kriterien der digitalen Souveränität bei der **Vergabe und Beschaffung** von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen,
- **Nutzung von offenen Standards** durch die Produktentwickler, damit die Verantwortlichen auch tatsächlich in die Lage versetzt werden, Anbieter und Produkte zu wechseln, wenn sie mit deren Produkten und Dienstleistungen die Datenschutzanforderungen nicht (mehr) oder nur ungenügend umsetzen können,
- **Veröffentlichung des Quellcodes und der Spezifikationen** öffentlich finanzierter digitaler Entwicklungen (siehe auch die Transparenzanforderung an algorithmische Systeme, Tz. 1.5),
- **Möglichkeiten zur Steuerung** des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung von Prozessen.

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22.09.2020: **Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen:**

https://www.datenschutzkonferenz-online.de/media/en/TOP 8 Entschließung digitale Souveränität_final.pdf

Kurzlink: *https://uldsh.de/tb39-2-1*

2.2 Verschlüsselung stärken statt schwächen

Ein Wiedergängerthema: Seit Jahrzehnten wird immer wieder vorgeschlagen, dass Möglichkeiten für Sicherheitsbehörden und Geheimdienste geschaffen werden sollen, um verschlüsselte Kommunikation mitzulesen. Und jedes Mal müssen wir die Argumente wiederholen: **Hintertüren oder von vornherein schwache Verschlüsselung sind keine Lösung** (z. B. 37. TB, Tz. 1.3 oder 38. TB, Tz. 2.3), sondern höhlen die Sicherheit aus. Denn Sollbruchstellen würden genutzt werden – und dies lässt sich nicht effektiv auf die „berechtigten Stellen“ beschränken.

Aus der DSK-Entschließung vom 25.11.2020:

„Eine sichere und vertrauenswürdige Verschlüsselung ist essenzielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung.“

Es wirkt manchmal wie eine Sisyphus-Aufgabe für die Datenschutzbeauftragten, bei Verantwortlichen, Auftragsverarbeitern oder Herstellern die technischen und organisatorischen Maßnahmen anzumahnen, um ein adäquates Schutzniveau zu gewährleisten. Auch simple und altbekannte Sicherheitsfehler werden regelmäßig wiederholt, die Menge der eingehenden Meldungen nach Artikel 33 DSGVO ist ein Indiz dafür, zumal davon auszugehen ist, dass die Dunkelziffer hoch ist. Die Digitalisierung schreitet voran: sowohl bei Unternehmen, die sich vor Wirtschaftsspionage und Angriffen auf die personenbezogenen Daten von Beschäftigten und Kundinnen und Kunden schützen müssen, als auch bei digitalen Verwaltungsdienstleistungen, die Bürgerinnen und Bürgern vertrauenswürdig angeboten werden sollen. In beiden Fällen gehören Ende-zu-Ende-Verschlüsselung zu dem Standardset an technischen und organisatorischen Maßnahmen. Doch wenn die Verschlüsselung nicht von einem zum anderen Ende (z. B. Verwaltung – Bürger, Unternehmen – Kunde) garantiert ist, sondern die Daten beim Transfer doch im Klartext sichtbar gemacht werden können, wird die Maßnahme entwertet, denn offensichtlich wirkt sie nicht.

Auch Verschlüsselung in Datenspeichern – eine der Maßnahmen, die im Zusammenhang mit dem EuGH-Urteil „Schrems II“ (Tz. 2.5, Tz. 11.5) als mögliche Abhilfe diskutiert wird – muss natürlich ihren Schutzzweck erfüllen, um die Risiken ausreichend eindämmen zu können. Eine nicht funktionierende Verschlüsselung, etwa mit eingebauten Hintertüren, bringt hier nicht die gewünschten Vorteile.

Auch sonst basieren viele datenschutzfreundliche Techniken zum Schutz der Vertraulichkeit, der Integrität oder der Datenminimierung auf der Anwendung geeigneter kryptografischer Verfahren. Solche „Privacy-Enhancing Technologies“ sind auch im Kontext von **Artikel 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)** wesentlich.

Wir plädieren dringend dafür, Verschlüsselung auszubauen und gegen Manipulationsversuche zu schützen. Allein die Diskussion, dass Staaten den Einbau von Hintertüren in Erwägung ziehen, führt bereits zu einem Vertrauensverlust der Menschen in staatlich bereitgestellte Software oder in Verwaltungsdienstleistungen.

Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 25.11.2020: **Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen:**

https://www.datenschutzkonferenz-online.de/media/en/TOP_29_Entschließung_Verschlüsselung.pdf

Kurzlink: *https://uldsh.de/tb39-2-2*

2.3 Der Ruf nach Harmonisierung – per Zentralisierung?

Über ein Jahr lang hatte die 16-köpfige Datenethikkommission der Bundesregierung – darunter auch die Landesbeauftragte für Datenschutz Schleswig-Holstein, Marit Hansen – Empfehlungen für den Einsatz algorithmischer Systeme und den Umgang mit Daten aus verschiedenen Perspektiven diskutiert.

Im Oktober 2019 hat die Datenethikkommission ihr umfangreiches Gutachten mit 75 Empfehlungen abgegeben. Man hätte nun erwartet, dass diese Empfehlungen unmittelbar nach der Veröffentlichung aufgegriffen, priorisiert und umgesetzt (oder mit fundierten Argumenten verworfen) würden, doch der Umsetzungsstatus ist bisher noch nicht zufriedenstellend.

Eine der 75 Empfehlungen hat allerdings dazu geführt, dass zahlreiche Diskussionen losgetreten wurden – zur **Zentralisierung der Datenschutzaufsicht im nichtöffentlichen Bereich**, denn dies habe ja die Datenethikkommission unter Beteiligung von zwei Datenschutzbeauftragten so gefordert. **Aber nein! Hier wurde (absichtlich?) eine Empfehlung der Datenethikkommission missverstanden.** In dem Gutachten steht nämlich etwas von einer erhöhten Wirkungskraft durch eine verbesserte Ausstattung und einer einheitlichen und kohärenten Anwendung des Datenschutzrechts.

> „Um die Wirkungskraft der Aufsichtsbehörden zu erhöhen, bedürfen diese einer weitaus besseren personellen und sachlichen Ausstattung. Sofern es nicht gelingt, die Abstimmung unter den deutschen Datenschutzaufsichtsbehörden zu verstärken und zu formalisieren und so die einheitliche und kohärente Anwendung des Datenschutzrechts zu gewährleisten, ist eine **Zentralisierung der Datenschutzaufsicht für den Markt** in einer – mit einem weiten Mandat ausgestatteten und eng mit anderen Fachaufsichtsbehörden kooperierenden – Behörde auf Bundesebene zu erwägen. Die Zuständigkeit der Landesdatenschutzbehörden für den öffentlichen Bereich soll hingegen unangetastet bleiben."

Dass dies in der jetzigen Struktur der Landesbeauftragten mit einer verstärkten Abstimmung einhergeht, überrascht nicht. Dieser **Abstimmungsprozess ist ohnehin notwendig im föderalen Europa** und geschieht ständig und mit kurzen Fristen im Europäischen Datenschutzausschuss.

Gutachten der Datenethikkommission (2019):

https://datenethikkommission.de/

Kurzlink: *https://uldsh.de/tb39-2-3a*

Wir sind **starke Befürworter klarer Regelungen und einheitlicher Rechtsauslegung**. Abweichende Meinungen unter den Aufsichtsbehörden in Bezug auf gleich gelagerte Fälle kommen – wie übrigens auch bei Gerichten – vor, sind aber selten. Meistens sind scheinbar gleiche Fälle doch nicht gleich und müssen verschieden behandelt werden. Wichtig ist der Austausch der Argumente und beispielsweise verschiedener Lösungsansätze. Auf dieser Basis und unter Berücksichtigung des Für und Wider ist es dann auch einfacher, einander mit guten Argumenten zu überzeugen.

In jedem Fall ist eine Präsenz der Datenschutzaufsicht in der Fläche nötig – demnach brauchte man zumindest Außenstellen in den Ländern oder Regionen. Die Landesbeauftragten für Datenschutz haben ohnehin die Aufsichtsfunktion im öffentlichen Bereich.

Dass es – und das gilt eigentlich für jede Konstellation auch außerhalb der Datenschutzbehörden – sicherlich Verbesserungspotenziale in der Zusammenarbeit sowohl im öffentlichen als auch nichtöffentlichen Bereich gibt, sehen wir sowohl für die europäische als auch für die deutsche Ebene. Dies zeigt sich beispielsweise darin, dass nicht jede Datenschutzaufsichtsbehörde **spezifische Expertise zu allen möglichen Technologien** vorhalten kann. Für den Akkreditierungs- und Zertifizierungsbereich haben wir daher eine **Verwaltungsvereinbarung** untereinander geschlossen, die auch Möglichkeiten der gegenseitigen Unterstützung und des freiwilligen Austauschs u. a. von Fachbegutachtenden vorsieht (Tz. 9.2). Aber auch für reguläre anlasslose oder anlassbezogene Prüfungen könnten spezifische Kenntnisse und Erfahrungen, über die nicht jede Behörde verfügt, von Nutzen sein: beispielsweise **Analysen von Verfahren der künstlichen Intelligenz, Quellcode-Sichtungen, forensische Begutachtungen, Konzepte der fortgeschrittenen Privacy-Enhancing Technologies**

oder Inspektionen von Hardwarekomponenten. Hinzu kommt der für den jeweiligen Prüfzweck geeignete **Aufbau von Prüflaboren** oder die Programmierung von **Prüftools vor Ort oder in Online-Prüfungen**.

Wer in den Protokollen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder stöbert, findet Informationen über eine **Arbeitsgruppe „DSK 2.0“**. In dieser Arbeitsgruppe geht es darum, die derzeitige Zusammenarbeit der Behörden einschließlich der Arbeitsweise der DSK zu evaluieren und gegebenenfalls Vorschläge für eine Neugestaltung zu erarbeiten.

https://www.datenschutzkonferenz-online.de/protokolle.html

Kurzlink: *https://uldsh.de/tb39-2-3b*

Art. 57 Abs. 1 Buchst. g DSGVO

(1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet […]

g) mit anderen Aufsichtsbehörden zusammenarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe leisten, um die einheitliche Anwendung und Durchsetzung dieser Verordnung zu gewährleisten;

Man muss auch nicht darauf warten, dass Verwaltungsvereinbarungen geschlossen oder gar Staatsverträge zwischen Ländern ausgehandelt werden: Amtshilfe untereinander gehört zu den Aufgaben der Datenschutzaufsichtsbehörde.

2.4 Impulse für den Beschäftigtendatenschutz

Beschäftigtendatenschutz gehört zu den Arbeitsfeldern der Datenschutzbeauftragten. Wir hatten erst im Jahr 2018 unsere Sommerakademie unter das Thema „Beschäftigtendatenschutz im digitalen Zeitalter“ gestellt und mit Expertinnen und Experten diskutiert (37. TB, Tz. 2.2.2 sowie Tz. 13.2). Auch im Projektbereich befassen wir uns mit Datenschutz in Arbeitswelten, besonders in Bezug auf den Einsatz von automatisierten Verfahren (Tz. 8.2). Das Thema ist deswegen diffizil und herausfordernd, weil die verschiedenen Beteiligten – besonders Arbeitgeber und Beschäftigte – jeweils eine ganze Reihe von berechtigten Interessen haben, die es abzuwägen gilt. Auf der einen Seite steht der **Schutz der Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz**, auf der anderen Seite die Verantwortlichkeit des Arbeitgebers für die Aufrechterhaltung des Betriebs einschließlich einer gewissen Fürsorgepflicht für alle Beschäftigte.

Die Digitalisierung im Beschäftigtenkontext und die zunehmende Verarbeitung personenbezogener Daten von Mitarbeiterinnen und Mitarbeitern führt zu zahlreichen Herausforderungen im Datenschutz. Die vorhandenen rechtlichen Regeln sind nicht immer einfach handhabbar. Schon aus Gründen der gewünschten Rechtssicherheit – und daran sollten alle Interesse haben – wären konkretere Regelungen in einem stimmigen Beschäftigtendatenschutzgesetz wünschenswert.

Art. 88 Abs. 1 DSGVO: Datenverarbeitung im Beschäftigungskontext

(1) Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.

Genau dies wird seit Jahrzehnten gefordert. Es hat immer wieder neue Anläufe für solche Gesetze und sogar schon Entwürfe für ein **Beschäftigtendatenschutzgesetz** gegeben, die jedoch dann irgendwo **stecken geblieben** sind.

Die DSGVO greift den Beschäftigtendatenschutz in Artikel 88 DSGVO auf und erlaubt dazu konkretisierende Rechtsvorschriften in den Mitgliedstaaten. In Deutschland wurde dies in § 26 BDSG umgesetzt – das reicht vielen Expertinnen und Experten aber nicht aus.

Auf Bundesebene sieht der Koalitionsvertrag einen Prüfauftrag zur Einführung eines eigenständigen Gesetzes zum Beschäftigtendatenschutz vor. Zu diesem Zweck hat das Bundesministerium für Arbeit und Soziales im Jahr 2020 einen Beirat eingerichtet, der auf Basis von Vorarbeiten, darunter auch der Impulse aus der Datenethikkommission (38. TB, Tz. 2.2), mögliche Inhalte eines solchen Gesetzes erörtert. **Der Bundesminister für Arbeit und Soziales, Hubertus Heil, hat die Landesbeauftragte für Datenschutz Schleswig-Holstein in diesen Beirat berufen.**

Zusammen mit weiteren Expertinnen und Experten, die für ihre Spezialfelder um Input in einzelnen Sitzungen gebeten werden, diskutiert der Beirat nicht nur vorhandene Defizite und rechtliche Regelungsoptionen, sondern hat den Blick für **verschiedene Instrumente** im Sinne eines Beschäftigtendatenschutzes geweitet. Auch effektive Möglichkeiten der Mitbestimmung bei komplexen Datenverarbeitungen können einen Beitrag leisten. Ausgehend von Konzepten wie Datenschutz „by Design“ muss man auch überlegen, wie technisch und organisatorisch die rechtliche Notwendigkeit des **Interessenausgleichs „by Design“** unterstützt werden kann.

Der Abschlussbericht des Beirats mit möglichst konkreten Empfehlungen wird für Mitte 2021 erwartet.

https://www.bmas.de/SharedDocs/Downloads/DE/Pressemitteilungen/2020/faktenblatt-beirat-zum-beschaeftigtendatenschutz.pdf

Kurzlink: *https://uldsh.de/tb39-2-4*

2.5 Es war einmal … der Privacy Shield: EuGH-Urteil „Schrems II“

Auch wenn man es schon lange kommen sah und keiner, der sich ein wenig mit Datenschutzfragen des grenzüberschreitenden Datentransfers beschäftigt hatte, wirklich überrascht sein konnte: Der EuGH hat mit seinem Urteil „Schrems II“ vom 16.07.2020 – C-311/18 erneut mit einem kleinen Paukenschlag ein **Datentransferinstrument für ungültig erklärt**: Nach Safe Harbor (EuGH-Urteil vom 06.10.2015 – C-362/14, „Schrems I“) traf es nun das Nachfolgemodell, den **EU-US Privacy Shield**.

Ebenso wie Safe Harbor bezeichnete der Privacy Shield eine Reihe von Regelungen, die US-amerikanische Unternehmen einzuhalten versprechen und im Anschluss auf einer Liste geführt werden. Eine wirkliche Überprüfung, z. B. durch unabhängige Dritte, fand nicht statt.

Der EuGH kritisiert insbesondere die **Massenüberwachung** durch die US-Geheimdienste, wovon die personenbezogenen Daten der europäischen Bürgerinnen und Bürger betroffen sind. Einen ausreichenden Rechtsschutz dagegen gibt es nicht, der angebotene Ombudsmechanismus kann dies nicht gewährleisten.

Mit Spannung war erwartet worden, ob der EuGH im selben Zuge auch ein weiteres häufig zum Einsatz kommendes Instrument kippt: die **Standarddatenschutzklauseln**. Dabei handelt es sich um von der EU-Kommission vorgegebene Standardverträge mit der Verpflichtung zur Einhaltung angemessener Datenschutzstandards. Während der Privacy Shield nur für den Datentransfer zwischen der EU und den USA verhandelt war, werden die Standarddatenschutzklauseln in Bezug auf alle möglichen Länder, die personenbezogene Daten erhalten, verwendet.

Im Ergebnis wurden die Standarddatenschutzklauseln nicht ebenfalls für unwirksam erklärt, denn der Datenexporteur kann nach Überzeugung des EuGH bei Zweifeln an der Rechtmäßigkeit den Datentransfer aussetzen. Dies wäre auch den zuständigen Datenschutzaufsichtsbehörden möglich, sollten sie Zweifel an der Rechtmäßigkeit haben.

Da mit Standardvertragsklauseln die Kritik der geheimdienstlichen Massenüberwachung nicht ausgeräumt werden kann, führte dies unmittelbar zu **Nachbesserungsnotwendigkeiten**. Die Arbeiten dazu auf Ebene der EU-Kommission, des Europäischen Datenschutzausschusses und der einzelnen Datenschutzaufsichtsbehörden sind noch nicht abgeschlossen.

Die Verantwortlichen sind aber unmittelbar in der Pflicht, die Rechtmäßigkeit ihrer Verarbeitung von personenbezogenen Daten – und damit auch der von ihnen eingebundenen Dienstleister – zu gewährleisten. Dazu gehört zunächst, sich einen **Überblick zu verschaffen**, wo überhaupt solche Datenübermittlungen stattfinden. Beispielsweise haben zahlreiche Verantwortliche auf ihren Webseiten einen Code eingebunden, der mit einem Datenfluss in die USA einhergeht. **Für jeden Datentransfer muss eine Rechtsgrundlage** – und Privacy Shield scheidet aus – **bestehen.** Ist keine Rechtsgrundlage ersichtlich, muss die Übermittlung unterbleiben. Manchmal stellen Verantwortliche fest, dass sie die betroffenen Dienste gar nicht benötigen – dann können sie ersatzlos wegfallen. Andernfalls muss man sich um **Alternativen** kümmern: Entweder der Dienstleister bessert selbst nach, oder man muss auf Konkurrenten ausweichen.

Auch technische Änderungen sind möglich, beispielsweise wenn der Personenbezug aus den übermittelten Daten entfernt wird und damit nur noch anonymisierte Daten transferiert werden. Weitere technische Lösungen wie Zugriffsbeschränkungen, Treuhändersysteme usw. können generell zur Risikoreduzierung zum Einsatz kommen. Die Frage der Zulässigkeit der Datenübermittlung ist aber getrennt zu klären (siehe auch Tz. 11.5).

Der Europäische Datenschutzausschuss hat **Fragen und Antworten zum EuGH-Urteil „Schrems II“** bereitgestellt:

https://edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_de

Kurzlink: *https://uldsh.de/tb39-2-5*

03

KERNPUNKTE

EuGH-Urteil zum Petitionsausschuss des Hessischen Landtages

Service für Abgeordnete

3 Landtag

Datenschutz und Informationsfreiheit betreffen auch die Abgeordneten als Mitglieder des Schleswig-Holsteinischen Landtages. Für das Jahr 2020 ist in diesem Zusammenhang über das Urteil des Europäischen Gerichtshofs zu Datenschutzfragen in einem Ausschuss des Hessischen Landtages zu berichten (Tz. 3.1). Außerdem weisen wir auf unseren Service für Abgeordnete hin, die in ihrer parlamentarischen Tätigkeit, als Privatpersonen oder auch in Bezug auf die Fragen, Beschwerden oder Hinweise, die Bürgerinnen und Bürger an sie gerichtet haben, die Möglichkeit haben, sich vertrauensvoll von uns beraten zu lassen (Tz. 3.2).

3.1 EuGH-Urteil zum Hessischen Petitionsausschuss

Gilt die Datenschutz-Grundverordnung auch für einen Petitionsausschuss? Im Fall des Hessischen Landtages hat der Europäische Gerichtshof (EuGH) dies bejaht: Mit dem Urteil vom 09.07.2020, C-272/19, wurde klargestellt, dass der Petitionsausschuss des Hessischen Landtages *„insoweit, als dieser Ausschuss allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als ‚Verantwortlicher' im Sinne von Art. 4 Nr. 7 der Verordnung 2016/679 einzustufen"* ist. Im konkreten Fall bedeutet dies, dass der Petitionsausschuss die Auskunftsanfrage des Petenten nach Artikel 15 DSGVO bearbeiten musste.

https://curia.europa.eu/juris/liste.jsf?language=de&num=C-272/19

Kurzlink: *https://uldsh.de/tb39-3-1a*

EuGH, Urteil vom 09.07.2020, C-272/19, Rn. 74

Nach alledem ist Art. 4 Nr. 7 der Verordnung 2016/679 dahin auszulegen, dass der Petitionsausschuss eines Gliedstaats eines Mitgliedstaats insoweit, als dieser Ausschuss allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als ‚Verantwortlicher' im Sinne dieser Bestimmung einzustufen ist, sodass die von einem solchen Ausschuss vorgenommene Verarbeitung personenbezogener Daten in den Anwendungsbereich dieser Verordnung, u. a. unter deren Art. 15, fällt.

Seit Veröffentlichung des Urteils wird in Bund und Ländern diskutiert, welche Ausstrahlung dieses Urteil auf Parlamente insgesamt hat. In dieser Situation hält die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder eine Überarbeitung des am 05.09.2018 getroffenen Beschlusses **„Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien"** für erforderlich. Mit Beschluss vom 22.09.2020 wurde daher der Beschluss aus dem Jahr 2018 zunächst ausgesetzt:

https://www.datenschutzkonferenz-online.de/media/dskb/TOP 6 Beschluss Anwendung der DSGVO auf die Datenverarbeitung von Parlamenten.pdf

Kurzlink: *https://uldsh.de/tb39-3-1b*

In vielen Landesdatenschutzgesetzen sind Formulierungen enthalten, die Aussagen zur „Wahrnehmung parlamentarischer Aufgaben" treffen, so auch in § 2 Abs. 3 LDSG SH.

§ 2 Abs. 3 LDSG

(3) Der Landtag, seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie die Landtagsverwaltung unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten. Der Landtag beschließt insoweit unter Berücksichtigung seiner verfassungsrechtlichen Stellung sowie der Grundsätze der Verordnung (EU) 2016/679 und dieses Gesetzes eine Datenschutzordnung.

Demnach fällt die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben nicht unter die Kontrolle der Landesbeauftragten für Datenschutz.

Als **Kontrollgremium** fungiert schon viele Jahre das **Datenschutzgremium des Schleswig-Holsteinischen Landtages**, das sich aus der sich aus Repräsentanten jeder im Landtag vertretenen Fraktion oder Gruppe zusammensetzt.

Informationen zu Datenschutz im Parlament:

https://www.landtag.ltsh.de/parlament/datenschutz-im-parlament/

Kurzlink: *https://uldsh.de/tb39-3-1c*

Das Datenschutzgremium hält jährlich mehrere Sitzungen ab, an denen die Landesbeauftragte für Datenschutz Schleswig-Holstein als Gast teilnimmt.

Was ist zu tun?

Es ist zu prüfen, inwieweit sich aus dem EuGH-Urteil Änderungsbedarfe in den aktuellen rechtlichen Regelungen ergeben.

3.2 Service für die Abgeordneten des Schleswig-Holsteinischen Landtages

Im letzten Tätigkeitsbericht haben wir die Beratungsmöglichkeit für Abgeordnete kurz vorgestellt (38. TB, Tz. 3.2). In diesem Sinne haben sich im Berichtsjahr einzelne Abgeordnete des Landtages und Mitglieder ihrer Teams bei der Landesbeauftragten für Datenschutz **vertrauensvoll beraten lassen**. Die Fragen, die an uns herangetragen wurden, umfassen eine große Spannbreite rechtlicher Einschätzungen zu vielfältigen Themen in den Bereichen **Datenschutz und Informationsfreiheit**.

Nicht überraschend ist die Tatsache, dass ein Großteil der Fragen die Pandemiesituation und Ideen oder Umsetzungen von konkreten Coronamaßnahmen betrafen.

Vielfach besteht zudem Beratungsbedarf zu technischen und organisatorischen Maßnahmen für die Praxis. In Einzelfällen werden wir auch um tiefgehendere technische Analysen gebeten.

Was ist zu tun?

Bei Fragen zu Datenschutz und Informationsfreiheit steht die Landesbeauftragte für Datenschutz den Abgeordneten des Schleswig-Holsteinischen Landtages mit ihrem Team gern zur Verfügung.

04

KERNPUNKTE

Coronamaßnahmen der Verwaltung – datenschutzgerecht

Prüfung eines kommunalen Rechenzentrums

Prüfungen der polizeilichen Datenverarbeitung

Datenpannen im Medizinbereich

4 Datenschutz in der Verwaltung

Die Landesbeauftragte für Datenschutz nimmt mit ihrer Dienststelle die Aufsicht über den Datenschutz in der Verwaltung wahr. Dazu gehört es insbesondere, Beschwerden von Bürgerinnen und Bürgern nachzugehen. Außerdem werden immer wieder Prüfungen bei verschiedenen Verantwortlichen durchgeführt, im Jahr 2020 waren dies z. B. die Prüfung eines kommunalen Rechenzentrums, Prüfungen im Polizeibereich und eine Prüfung einer Gesundheitseinrichtung. Außerdem gibt die Landesbeauftragte für Datenschutz schriftlich und mündlich Stellungnahmen zu Gesetzgebungsvorhaben des Landtages ab.

In diesem Kapitel werden für das Berichtsjahr die Tätigkeiten der Landesbeauftragten für Datenschutz in den Bereichen der allgemeinen Verwaltung einschließlich Schule, Pflegeberufekammer und Feuerwehr (Tz. 4.1), Polizei (Tz. 4.2), Justiz (Tz. 4.3), Soziales (Tz. 4.4) und Medizin (Tz. 4.5) beschrieben. Wie überall spielten Fragen rund um die Coronapandemie eine große Rolle, sowohl bezüglich spezieller Maßnahmen (Tz. 4.1.1, Tz. 4.1.2 und Tz. 4.3.2) als auch in Bezug auf die zunehmende Digitalisierung (z. B. Tz. 4.1.5, siehe auch Kapitel 6).

4.1 Allgemeine Verwaltung

4.1.1 Verwendung eines Fragebogens zur Coronaprävention

Auf Grundlage des Hinweises eines Bürgers erhielt das ULD Kenntnis, dass eine Kommune den Zutritt zum Rathaus von der Ausfüllung eines Fragebogens abhängig machte. Vor dem Hintergrund der steigenden Infektionszahlen sollte der Hinweisgeber eine Selbsteinschätzung zu seinem Gesundheitszustand abgeben und hierzu verschiedene Fragen gewissenhaft beantworten. Der Zweck der Datenerhebung bestand nach den Angaben im Fragebogen allerdings nicht vordergründig darin, mögliche Infektionen in den Räumlichkeiten des Rathauses zu vermeiden, sondern es sollte die Ausbreitung des Coronavirus im Gemeindegebiet eingeschränkt und verlangsamt werden.

Die öffentliche Stelle bat die Besucherinnen und Besucher zunächst um Angaben zu Name, Vorname, Anschrift und Telefonnummer, was zusätzlich mit Datumsangabe und Unterschrift zu unterzeichnen war. Weiterhin wurde dazu aufgefordert, der Gemeinde mitzuteilen, ob in den letzten zwei Wochen ein Aufenthalt außerhalb von Deutschland erfolgte. Ferner erfragte die Kommune, ob wissentlich ein persönlicher Kontakt zu einer Person bestand, bei welcher ein Labor das Coronavirus nachwies. Schließlich sollte ein Ankreuzen mit „ja“ oder „nein“ erfolgen, ob derzeit grippeähnliche Symptome (z. B. Husten, Schnupfen, Kratzen im Hals, Fieber, Probleme beim Atmen) bestehen.

Sobald an einer Stelle „ja“ angekreuzt wurde, war es den Besucherinnen und Besuchern laut Hinweis im Fragebogen verwehrt, das Rathaus zu betreten.

Die Gemeinde erhielt in einem daraufhin eröffneten datenschutzrechtlichen Prüfverfahren die Gelegenheit, sich zu dem verwendeten Fragebogen zu äußern. Maßgeblich waren dabei vor allem folgende Punkte:

- Es blieb offen, zu welchem konkreten Zweck eine Erhebung der Daten mittels des Fragebogens erfolgte. Nach den datenschutzrechtlichen Vorgaben müssen aber die Verarbeitungszwecke eindeutig formuliert sein.
- Weiterhin blieb unklar, auf welcher Rechtsgrundlage die Daten erhoben wurden. Von Bedeutung war dabei, dass dort bei der Abfrage grippeähnlicher Symptome Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO erhoben werden, deren Verarbeitung nur auf Grundlage einer besonderen Ermächtigung nach Art. 9 Abs. 2 DSGVO zulässig ist.
- Bezüglich der Erhebung von Angaben zum Aufenthalt in den letzten zwei Wochen und den wissentlich persönlichen Kontakten mit Personen, bei denen das Coronavirus im Labor nachgewiesen wurde, ist ein Abstellen auf eine Befugnis nach Art. 6 Abs. 1 Buchst. c oder e DSGVO nicht möglich. Insbesondere

ergeben sich die Verpflichtungen zur Erhebung von Kontaktdaten abschließend aus der jeweils gültigen Landesverordnung zur Bekämpfung des Coronavirus SARS-CoV-2 des Landes-Schleswig-Holstein (Corona-BekämpfV).

- Es blieb fraglich, ob die Verwendung eines Fragebogens zur Erreichung des verfolgten Zwecks geeignet ist. Dabei müssten zunächst ausschließlich wahrheitsgemäße Angaben in den Fragebögen enthalten sein. Weiterhin müsste die Gemeinde jede Zutrittsberechtigung einzeln prüfen und die Fragebögen sofort auswerten, was mit einem zusätzlichen Aufwand verbunden ist. Als weniger eingriffsintensive Maßnahme anstelle einer Erhebung persönlicher Angaben mittels Fragebogen wäre z. B. die Bereitstellung von Aushängen in Betracht zu ziehen, wo um ein Absehen von Besuchen gebeten wird, falls entsprechende Fragen innerlich mit „ja“ beantwortet werden müssten.
- Bezüglich der Fragebögen hätte die Gemeinde auch eine konkrete Frist für die Aufbewahrung der Fragebögen bestimmen müssen. Personenbezogene Daten sind insbesondere dann zu löschen, wenn der jeweilige Erhebungszweck erfüllt ist.
- Im Falle der Verwendung von Fragebögen müssten die Besucherinnen und Besucher auch pflichtgemäß nach Artikel 13 DSGVO unterrichtet werden, d. h., die Gemeinde hat die Verpflichtung, vor allem die Zwecke der Verarbeitung, die Aufbewahrungsdauer für die Fragebögen, etwaige Empfänger der Daten und z. B. Angaben zur Wahrnehmung von Rechten nach der DSGVO mitzuteilen.

Die Gemeinde hat im datenschutzrechtlichen Prüfverfahren umgehend Stellung genommen und mitgeteilt, dass künftig auf die Verwendung des Fragebogens verzichtet wird und vorhandene Fragebögen vernichtet werden. Das ULD hat der Gemeinde Hinweise zum datenschutzkonformen Umgang mit Fragebögen erteilt.

Was ist zu tun?

Die Verwendung eines Fragebogens in der geschilderten Form entspricht nicht den datenschutzrechtlichen Anforderungen. Im konkreten Fall war dieses Vorgehen nicht geeignet, der Ausbreitung des Coronavirus präventiv entgegenzuwirken. Den Kommunen wird empfohlen, bei der Konzipierung von Präventionsmaßnahmen stets die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten einzubeziehen.

4.1.2 Temperaturmessung bei Rathausbesuchen

Im Rahmen einer Beschwerde wurde vorgetragen, dass am Eingang des Rathauses einer Gemeinde ein Temperaturmessgerät aufgestellt worden sei. Personen, bei denen eine Körpertemperatur von über 37 Grad festgestellt wird, würde der Zutritt zum Rathaus versagt werden. Hintergrund sei eine Maßnahme zur Coronaprävention. Zudem würde das Gerät einen Signalton absetzen, sodass umstehende Personen Kenntnis von der erhöhten Körpertemperatur der getesteten Person erhielten.

Im eingeleiteten Beschwerdeverfahren führte die Gemeinde aus, dass ein Temperaturscanner zur Messung der Körpertemperatur im Eingangsbereich des Rathauses bereitstehe. Die Nutzung des Geräts erfolge aber nur auf freiwilliger Basis. Personen, die von dieser freiwilligen Möglichkeit keinen Gebrauch machten, werde der Zutritt zum Rathaus nicht versagt. Der Einsatz einer akustischen Warnanlage mit Signalton wurde zwar bestätigt, jedoch sei der Warnton nur für den freiwilligen Nutzer hörbar gewesen. Die Tonfunktion schaltete die Gemeinde vorsorglich ab. Weiterhin erläuterte die Gemeinde, dass nach der Nutzung des Temperaturscanners keine Speicherung von Messergebnissen erfolge. Es gebe auch keine manuelle Protokollierung gemessener Temperaturen oder einen Mitschnitt per Videoaufzeichnung.

Die Aufstellung des Temperaturmessgeräts begründete die Gemeinde mit Fürsorgepflichten gegenüber den Bürgerinnen und Bürgern sowie den Mitarbeiterinnen und Mitarbeitern des Rathauses im Zusammenhang mit der Coronapandemie. Die Sicht auf das Temperaturmessgerät schränkte die Gemeinde durch Aufstellung einer Stellwand ein, wodurch nur der freiwillige Nutzer Kenntnis von dem Messergebnis erhält. Das Gerät wird zwischenzeitlich von der Gemeinde nicht weiter eingesetzt.

Anlass zur Prüfung gab vor allem die Frage, ob es sich bei der Gemeinde um den datenschutzrechtlich Verantwortlichen handelt. Der Verantwortliche muss eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten vorweisen können; zudem entstehen Informationspflichten gegenüber den Nutzerinnen und Nutzern des Messgeräts. Die Verantwortlichkeit ist nicht davon abhängig, dass Zugriffsmöglichkeiten für die personenbezogenen Daten bestehen oder die Gemeinde von den Testergebnissen Kenntnis erhält. Weiterhin ist die fehlende Speicherung der Daten unerheblich. Es erfolgt zumindest eine zurechenbare Datenerhebung. Ausreichend ist eine Handlung, die eine Temperaturmessung bei den Personen ermöglicht, wobei die Gemeinde auch ein Interesse daran hat, dass den Nutzerinnen und Nutzern ihre Testergebnisse bekannt gegeben werden. Die Gemeinde hat durch die Bereitstellung des Messgeräts die Erhebung personenbezogener Daten erst ermöglicht. Die Gemeinde verfolgte mit der Ermittlung der Testergebnisse auch einen Zweck, in diesem Fall die Erfüllung von Fürsorgepflichten. Auch wenn die Gemeinde die Ergebnisse nicht einsehen konnte, überließ diese das Messgerät am Eingang des Rathauses nicht ohne eine eigene Intention einem Dritten zur Eigennutzung. Vor diesem Hintergrund ist die Annahme einer datenschutzrechtlichen Verantwortlichkeit nicht ausgeschlossen.

Bezüglich der Körpertemperatur handelt es sich um Gesundheitsdaten, die einem besonderen Schutz unterliegen. Das ULD empfahl der Gemeinde insbesondere, im Falle der weiteren Nutzung des Geräts die Erfüllung der Informationspflichten mithilfe eines Aushangs umzusetzen. Hierdurch könnten die Besucherinnen und Besucher des Rathauses u. a. darüber unterrichtet werden, dass keine Speicherung der Daten erfolgt und ausschließlich eine freiwillige Nutzung des Temperaturmessgeräts vorgesehen ist. Außerdem könnten sie per Aushang über die konkreten Zwecke für den Einsatz des Geräts und die zugrunde liegende Rechtsgrundlage für eine Messung der Körpertemperatur informiert werden.

Was ist zu tun?

Bei Maßnahmen zur Coronaprävention mit Verarbeitung personenbezogener Daten müssen die Verantwortlichen insbesondere eine Rechtsgrundlage für die verfolgten Zwecke benennen können und die Transparenzpflichten umsetzen.

4.1.3 Ton- und Videoaufnahmen in kommunalen Sitzungen

Das ULD erhielt im Berichtszeitraum Anfragen von Gemeinden hinsichtlich der Umsetzung von Ton- und Videoaufnahmen in kommunalen Sitzungen. Ausgangspunkt sind gesetzliche Bestimmungen in der Gemeindeordnung und in der Kreisordnung, die zur Thematik eine Regelung enthalten. Erforderlich ist damit eine Bestimmung in der Hauptsatzung. Sollte eine solche Regelung geschaffen werden, so müssten zusätzlich die Vorgaben nach der DSGVO beachtet werden. Diese Vorgaben könnten durch Satzungsrecht nicht beschränkt werden.

§ 32 Abs. 4 Gemeindeordnung

Unbeschadet weiter gehender Berechtigungen aus anderen Rechtsvorschriften kann die Hauptsatzung bestimmen, dass in öffentlichen Sitzungen Film- und Tonaufnahmen durch die Medien oder die Gemeinde mit dem Ziel der Veröffentlichung zulässig sind.

Sind Medienvertreter die Verantwortlichen für die Datenverarbeitung, so müssen diese vor allem eine Rechtsgrundlage für die Datenverarbeitung belegen können, gegebenenfalls datenschutzrechtliche Transparenzpflichten einhalten und Widersprüche gegen die Anfertigung von Filmaufnahmen beachten. Vorschriften der Gemeindeordnung können deren Datenverarbeitung nicht pauschal legitimieren.

Erfolgt die Verarbeitung durch die Gemeinde als Verantwortliche, so müssen insbesondere die Anwesenden vorab u. a. über die Aufzeichnungszwecke, die Rechtsgrundlagen und die Veröffentlichungs- sowie Speicherdauer (Art. 13 Abs. 1 und 2 DSGVO) aufgeklärt werden, da eine Datenerhebung bei den betroffenen Personen erfolgt. Es müsste außerdem festgelegt werden, zu welchem konkreten Zweck (Art. 5 Abs. 1 Buchst. b DSGVO) die Anfertigung und Veröffentlichung der Aufnahmen erfolgen soll (z. B. Kenntnisnahme von den Beratungen und Beratungsergebnissen bis zur Anfertigung des Sitzungsprotokolls).

In § 35 Abs. 4 GO wird keine Aussage zur Veröffentlichungs- und Speicherdauer getroffen. Zu beachten ist der Datenschutzgrundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO). Demnach müssen personenbezogene Daten dem Zweck angemessen und erheblich und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Damit korrespondiert auch das Gebot einer möglichst frühzeitigen Löschung (Art. 5 Abs. 1 Buchst. e DSGVO). Eine Löschung von Film- und Tonaufnahmen muss erfolgen, wenn der Aufzeichnungszweck erfüllt ist (z. B. Fertigstellung/Bestätigung des Protokolls in der nächsten Sitzung).

Geregelt werden sollte daher auch eine möglichst kurze Veröffentlichungsfrist, die den Bürgerinnen und Bürgern noch eine angemessene Kenntnisnahme ermöglicht, wobei im Falle der zwischenzeitlichen Einstellung eines Sitzungsprotokolls eine frühzeitigere Beendigung der Veröffentlichung in Betracht kommt. Eine darüber hinausgehende Speicherung von Film- und Sprachaufnahmen wird nach der Zweckerfüllung nicht zulässig sein.

Zu beachten ist, dass § 35 Abs. 4 GO nur öffentliche Sitzungen erwähnt. Nichtöffentliche Sitzungen werden nicht erfasst.

In § 35 Abs. 4 GO wird dem Wortlaut nach keine Verpflichtung zur Anfertigung von Aufnahmen aus öffentlichen Sitzungen mit dem Ziel der Veröffentlichung eingeführt. Vielmehr wird eine allgemeine Zulässigkeit solcher Veröffentlichungen angesprochen. Die Gemeinde benötigt für die beabsichtigte Datenverarbeitung Rechtsgrundlagen, die sich aus der DSGVO in Verbindung mit dem LDSG ergeben können. Zu diesen Rechtsgrundlagen zählt etwa die Einwilligung. Hierfür sind die Vorgaben nach Artikel 7 DSGVO einzuhalten, was auch die Freiwilligkeit der Erklärung und die Belehrung über die jederzeitige Widerrufbarkeit der Einwilligung umfasst. Zusätzlich sind u. a. auch hier die Pflichtinformationen nach Art. 13 Abs. 1 und 2 DSGVO zu erteilen.

Bei der Suche nach einer Rechtsgrundlage kommen außerdem Art. 6 Abs. 1 Buchst. c und e DSGVO in Betracht: Art. 6 Abs. 1 Buchst. c DSGVO wäre maßgeblich, wenn die Gemeinde auf Grundlage einer Bestimmung die Verpflichtung hätte, bestimmte Aufnahmen mit dem Ziel der Veröffentlichung anzufertigen. Nach Art. 6 Abs. 1 Buchst. e DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Die Aufgabe müsste allerdings näher erläutert werden, wobei wiederum der Zweck der Anfertigung und Veröffentlichung der Aufnahmen konkret zu beschreiben ist. Die Vorschrift allein reicht als Rechtsgrundlage nicht aus. Vielmehr muss sich die konkrete Aufgabenbeschreibung aus einer anderen Norm ergeben.

Was ist zu tun?

Die Gemeinden und Kreise müssen in Bezug auf die Anfertigung und Weiterverarbeitung von Ton- und Videoaufnahmen die Vorgaben der DSGVO einhalten. Die Vorschriften der Gemeindeordnung und der Kreisordnung ersetzen nicht die datenschutzrechtlichen Verpflichtungen, wonach auch angemessene technische und organisatorische Maßnahmen zu treffen sind.

4.1.4 Veröffentlichung der Kontaktdaten von Gemeindevertreterinnen und -vertretern

In einer Gemeinde stellte sich die Frage, ob im kommunalen Webauftritt die Veröffentlichung von Kontaktdaten der Gemeindevertreterinnen und Gemeindevertreter, eingeschlossen Wohnadresse sowie private Telefonnummer und E-Mail-Adresse, zulässig ist.

Die Gemeinde ist die Betreiberin des Webauftritts und damit datenschutzrechtlich Verantwortlicher für die betroffene Verarbeitung personenbezogener Daten. Damit muss die Gemeinde die Rechenschaftspflichten nach der DSGVO einhalten und belegen können, auf welcher rechtlichen Grundlage sie die Kontaktdaten der Gemeindevertreterinnen und Gemeindevertreter öffentlich zugänglich bereitstellt.

Die Namen von Gemeindevertreterinnen und Gemeindevertretern und Angaben zu deren beruflicher Tätigkeit sind bereits nach den Vorschriften der Gemeindeordnung zu veröffentlichen.

§ 32 Abs. 4 Satz 1 und 2 Gemeindeordnung

Die Mitglieder der Gemeindevertretung, der Ortsbeiräte und der Ausschüsse haben der oder dem Vorsitzenden der Gemeindevertretung ihren Beruf sowie andere vergütete oder ehrenamtliche Tätigkeiten mitzuteilen, soweit dies für die Ausübung ihres Mandats von Bedeutung sein kann. Die Angaben sind zu veröffentlichen.

Der Veröffentlichungsort wird gesetzlich nicht geregelt. Es liegt aber nahe, dass die Veröffentlichung (auch) im Webauftritt der Gemeinde erfolgt. Mit dem Vorsitz der Gemeindevertretung könnte aber Rücksprache gehalten werden, ob gegebenenfalls nähere Regelungen in der Geschäftsordnung der Gemeindevertretung getroffen wurden. Bestand Einigkeit, dass der Webauftritt der Gemeinde hierfür in Anspruch zu nehmen ist, so wäre die Veröffentlichung der Namen der Gemeindevertreterinnen und Gemeindevertreter in diesem Medium nicht zu beanstanden.

Bezüglich der Angaben zu privaten Anschriften, Telefonnummern und E-Mail-Adressen besteht keine gesetzliche Befugnis. Soweit daher keine solchen Vorschriften eine Veröffentlichung vorsehen, wäre eine Einwilligung der Gemeindevertreterinnen und Gemeindevertreter zur Veröffentlichung dieser zusätzlichen Daten einzuholen. Datenschutzrechtliche Einwilligungen bedürfen keiner Schriftform. Allerdings sollte die Gemeinde beim Verzicht auf eine schriftliche Einwilligungserklärung das mündliche Einverständnis dokumentieren. Auf diese Weise kann die Gemeinde bestehende Rechenschaftspflichten einhalten. Bei Einwilligungserklärungen ist schließlich auch darauf zu achten, dass der Zweck und das bestimmte Veröffentlichungsmedium sowie die konkreten einzelnen Daten bezeichnet werden. Die Gemeinde muss auch auf die Freiwilligkeit einer Einwilligung und deren jederzeitige Widerruflichkeit hinweisen.

Was ist zu tun?

Hinsichtlich der Verarbeitung von Kontaktinformationen der Gemeindevertretung ist zu differenzieren. Bezüglich der Veröffentlichung privater Anschriften, Telefonnummern und E-Mail-Adressen sind die Voraussetzungen einer Einwilligung zu prüfen.

4.1.5 Digitale Schule – ja, aber datenschutzkonform

Mit den Mitteln aus dem Digitalpakt beschleunigt sich auch in den Schulen in Schleswig-Holstein die Digitalisierung des Unterrichts. Bedingt durch die Coronapandemie und das dadurch ausgelöste Distanzlernen mussten das Bildungsministerium und auch das Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein (IQSH) schnell für leidlich funktionierende Ad-hoc-Lösungen sorgen, statt – wie eigentlich geplant – die Ausstattung der Schulen mit digitalen Mitteln wie z. B. Lernmanagementsystemen, Online-Speichern und anderen Online-Angeboten von Anfang an unter vollständiger Beachtung aller (datenschutz-)rechtlichen Vorgaben zu konzipieren.

So wurde ein Lernmanagementsystem zunächst für ein Jahr beschafft, das allen Schulen vom Bildungsministerium kostenfrei zur Nutzung zur Verfügung gestellt wird. Der zentrale Datenschutzbeauftragte für die öffentlichen Schulen hat dabei auf die Datenschutzkonformität dieses Systems geachtet. Die Medienberatung des IQSH hat dafür gesorgt, dass auf die Schnelle Empfehlungen für andere digitale Produkte gegeben wurden. Eine Schwierigkeit bestand allerdings nicht nur in Schleswig-Holstein darin, bei den sich ständig in Funktionalität, Sicherheit und Datenschutzaspekten verändernden Dienstleistungen und Softwareprodukten alles ausreichend im Blick zu haben.

Zudem waren die schulrechtlichen Regelungen nicht auf komplette oder partielle Schulschließungen und die Notwendigkeit, zur Kompensation des fehlenden Präsenzunterrichts digitale Lehr- und Lernmittel einzusetzen, vorbereitet. So enthält das Schulgesetz Schleswig-Holstein bisher keine Vorschriften im Hinblick auf digitale Lehr- und Lernmittel, sondern kennt z. B. lediglich analoge Schulbücher.

Auch wenn sich das Bildungsministerium bemüht hat, bei der Bereitstellung und Förderung digitaler Lehr- und Lernmittel die datenschutzrechtlichen Vorschriften nicht aus dem Blick zu verlieren, besteht die Gefahr, dass sich ungeordnet in einigen Schulen IT-Verfahren zum Distanzlernen etabliert haben, die einer datenschutzrechtlichen Überprüfung nicht standhalten würden. Es ist deshalb dringend geboten, eine Bestandsaufnahme durchzuführen, um zu gewährleisten, dass in allen Schulen die datenschutzrechtlichen Vorschriften eingehalten werden und es nicht zu einer rechtswidrigen Verarbeitung personenbezogener Daten von Schülerinnen, Schülern und Lehrkräften kommt.

Was ist zu tun?

Das Bildungsministerium sollte sich durch eine Abfrage bei allen Schulen einen Überblick darüber verschaffen, welche digitalen Lehr- und Lernmittel im Jahre 2020 beschafft wurden und noch beständig eingesetzt werden. Sofern Schulen IT-Verfahren einsetzen, die einer datenschutzrechtlichen Überprüfung nicht standhalten, muss dies unverzüglich beendet werden. Im Schulgesetz Schleswig-Holstein sollten Regelungen zum Einsatz von digitalen Lehr- und Lernmitteln aufgenommen werden.

4.1.6 Einheitliche Schulverwaltung und Schulportal

Auf Initiative des Bildungsministeriums und gestützt auf einen Landtagsbeschluss aus dem Jahr 2019 wird den Schulverwaltungen ein IT-Verfahren (School-SH) zur Verarbeitung der Daten der Schülerinnen, Schüler und Eltern kostenfrei zur Verfügung gestellt. Ziel ist es, dass alle Schulen in Schleswig-Holstein dieses Verfahren nutzen, damit die Uneinheitlichkeit der bisher an den Schulverwaltungen eingesetzten Verwaltungsverfahren beendet wird. Standardisierte Lösungen bieten den Vorteil, dass sie mit weniger Aufwand betrieben und weiterentwickelt werden können. Dies betrifft auch die notwendigen Anpassungen, wenn Fehler oder Sicherheitslücken gefunden werden.

Wir haben den Aufbau des IT-Verfahrens zur einheitlichen Schulverwaltung auf Wunsch des Bildungsministeriums von Anfang an begleitet. Im Rahmen dieser konstruktiven Zusammenarbeit mit dem Projektmanagement konnten wir sicherstellen, dass die datenschutzrechtlichen Vorschriften des Schulgesetzes, der Schul-Datenschutzverordnung und der DSGVO umfassend berücksichtigt wurden.

Eine ähnliche datenschutzrechtliche Begleitung konnten wir bezüglich des Schulportals leisten. Das Schulportal wird den Schülerinnen, Schülern und Lehrkräften webbasiert den Zugang zu digitalen Lehr- und Lernmitteln, wie z. B. Lernmanagementsystemen, ermöglichen. Zusätzlich wird darüber hinaus der Zugang der Lehrkräfte zu ihren dienstlichen E-Mail-Postfächern möglich sein. Ferner soll über das Schulportal für die Lehrkräfte auch ein Zugang zu den Daten der von ihnen unterrichteten Schülerinnen und Schüler in School-SH ermöglicht werden. Dieser Zugang wird mit einer Zwei-Faktor-Authentifizierung abgesichert.

Das ULD wird sich mit diesen Schulverfahren weiterhin intensiv beschäftigen.

4.1.7 Datenschutz in der Pflegeberufekammer Schleswig-Holstein – vergessen?

Mit dem Gesetz über die Kammer und die Berufsgerichtsbarkeit für die Heilberufe in der Pflege vom 16.07.2015 wurde auch die Errichtung der Pflegeberufekammer als Körperschaft des öffentlichen Rechts eingeleitet. Damit trat der seltene Fall ein, dass eine neue öffentliche Stelle geschaffen wurde, die in großem Umfang personenbezogene Daten betroffener Personen verarbeiten soll. Man hätte zu diesem Zeitpunkt erwarten können, dass beim Aufbau der Verwaltung der Pflegeberufekammer von vornherein die seinerzeit bestehenden datenschutzrechtlichen Vorgaben insbesondere im Hinblick auf die zu ergreifenden technischen und organisatorischen Maßnahmen beachtet würden. Man hätte insbesondere die Möglichkeit gehabt, von Anfang an die gesamte Verwaltungsorganisation datenschutzkonform auszurichten.

Beim Aufbau der Pflegeberufekammer Schleswig-Holstein wurde der Datenschutz augenscheinlich jedoch komplett vergessen. Das ULD war mit einer Vielzahl von Beschwerden gegen die Datenverarbeitung der Pflegeberufekammer befasst. Insbesondere wurden keine oder keine vollständigen Auskünfte nach Artikel 15 DSGVO erteilt. In einem aufsichtsbehördlichen Verfahren überprüften wir einige grundsätzliche Vorgaben der Datenverarbeitung.

Die bisher im Rahmen des durchgeführten Anhörungsverfahrens gewonnenen Erkenntnisse lassen ein unschönes Bild erkennen. Der Pflegeberufekammer war z. B. anscheinend noch nicht einmal bekannt, aufgrund welcher Rechtsgrundlagen die personenbezogene Datenverarbeitung ihrer Mitglieder und ihrer eigenen Mitarbeitenden erfolgt. Das ist aber Voraussetzung für jede Verarbeitung personenbezogener Daten. Für die verwendete elektronische Datenverarbeitung konnte die Pflegeberufekammer keine den datenschutzrechtlichen Anforderungen genügende Dokumentation vorlegen. Diese hätte jedoch bereits vor Inbetriebnahme vorliegen müssen.

Als Zwischenfazit ist die Feststellung zu treffen, dass sich bei der Einrichtung der Pflegeberufekammer augenscheinlich niemand mit Kompetenz und Fachwissen um die zu beachtenden datenschutzrechtlichen Vorschriften und deren Umsetzung gekümmert hat.

Was ist zu tun?

Die bisher festgestellten datenschutzrechtlichen Mängel sind unverzüglich abzustellen.

4.1.8 Wenn Berufsfeuerwehrleute zu Filmstars werden

Aufgrund einer Beschwerde ist uns bekannt geworden, dass eine in Schleswig-Holstein im Einsatz befindliche Berufsfeuerwehr bei ihren Einsätzen von einem Filmteam begleitet wird. Dieses Filmteam erstellt Aufnahmen vom Alltag der Berufsfeuerwehrleute und den damit einhergehenden Einsätzen. Augenscheinlich werden dabei auch Szenen aufgenommen, in denen Personen zunächst gefilmt und dann erst gefragt werden, ob sie offen oder in anonymisierter (verpixelter) Form im Filmbeitrag gezeigt werden dürfen. Um die Einsatzhandlungen der Feuerwehrleute noch intensiver und einsatznäher im Bild festzuhalten, trugen die Feuerwehrleute auch Bodycams, die der Filmfirma gehören. Diese Aufnahmen wurden ebenfalls von der Filmfirma ausgewertet und für die Einsatzstorys verwendet. Man stelle sich einen Einsatz im brennenden Haus vor, wenn die Personen, die zur Rettung der Bewohnerinnen und Bewohner herbeieilen, gleich jeden Schritt und Handschlag filmen und dabei natürlich auch verzweifelte Menschen und ihre Privaträume ins Bild geraten können.

Hinsichtlich der datenschutzrechtlichen Zulässigkeit solcher Filmaufnahmen, in denen erst aufgezeichnet und dann erst die betroffenen Personen gefragt werden, argumentiert die Berufsfeuerwehr dahin gehend, dass dies im Rahmen des Landespressegesetzes zulässig sei. Aus unserer Sicht ist es jedoch zweifelhaft, ob eine solche Datenverarbeitung auf die Pflicht zur Zusammenarbeit mit der Presse nach dem Landespressegesetz gestützt werden kann.

Wir haben einen Hinweis erteilt, dass eine zeitgleiche Begleitung der Berufsfeuerwehr durch das Filmteam einen Verstoß gegen die DSGVO darstellen kann, wenn dabei personenbezogene Daten betroffener Personen offenbar werden können. Im Hinblick auf den Einsatz von Bodycams haben wir eine Warnung ausgesprochen, weil keine Rechtsgrundlage ersichtlich ist, die einen Einsatz erlauben würde.

Was ist zu tun?

Das Datenschutzrecht gilt auch bei Feuerwehreinsätzen. Das bedeutet in diesem Fall: keine Bodycams im Feuerwehreinsatz, wenn Menschen davon betroffen sein können.

4.1.9 E-Mail-Versand von Gebührenbescheiden durch die Abfallwirtschaft

Ein von einem Kreis mit der Durchführung und Organisation der Abfallentsorgung beauftragter Betrieb plante die Versendung von Rechnungen und Abfallgebührenbescheiden per E-Mail. Der Kreis betraute den Abfallwirtschaftsbetrieb auch mit der Veranlagung und dem Versand der Gebührenbescheide. Die Bescheide enthalten erwartungsgemäß personenbezogene Daten der Gebührenschuldner, im Einzelnen Angaben zu Name, Vorname und Anschrift, gegebenenfalls Kontaktdaten eines Empfangsbevollmächtigten, Angaben dazu, welche Behälter mit welchem Leerungsrhythmus der Betrieb vorhält, die Höhe der Jahresgebühr oder des Jahresentgelts, Informationen zur Fälligkeit der Forderung und bei einem erteilten SEPA-Lastschriftmandat die letzten drei Ziffern der IBAN.

Der Kunde wird im Webauftritt des Abfallwirtschaftsbetriebs auf die Möglichkeit des Erhalts von Rechnungen oder Gebührenbescheiden per E-Mail hingewiesen. Zum Einsatz kommt eine Transportverschlüsselung. Entscheidet sich der Kunde für den Versand per E-Mail, wird dieser in einer Eingabemaske zur Bereitstellung einiger Daten gebeten, um sich zu verifizieren. Die Anmeldeprozedur soll die Übermittlung einer Bestätigungs-E-Mail enthalten, in welcher der Kunde zum Abschluss der Anmeldung einen Bestätigungslink anklicken muss.

Die skizzierte Verfahrensweise hat das ULD geprüft und keine durchgreifenden datenschutzrechtlichen Mängel an der Konzeption festgestellt. Zu diesem Ergebnis gelangte das ULD auch, weil der Entwurf

eine Beachtung und Umsetzung der Vorgaben der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ der DSK vorsah. Das entsprechende Dokument enthält insbesondere Ausführungen zu den technischen Anforderungen bei der Erbringung von E-Mail-Diensten, zu den Sorgfaltspflichten bei der Auswahl von Diensteanbietern, Fallgruppen des E-Mail-Versands mit Risikoeinstufungen sowie Anforderungen an Verschlüsselungs- und Signaturverfahren. Die Orientierungshilfe ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/oh/20200526_orientierungshilfe_e_mail_verschluesselung.pdf

Kurzlink: *https://uldsh.de/tb39-4-19*

Der Abfallwirtschaftsbetrieb erhielt für die weitere Konzeption noch Hinweise, wonach die Kunden einen geeigneten Zugang zu den Pflichtinformationen (Artikel 13 DSGVO) erhalten müssen. Ferner ist durch eine deutliche Hervorhebung sicherzustellen, dass eine echte Wahlmöglichkeit zwischen papiergebundenen Bescheiden bzw. Rechnungen und einer Übersendung per E-Mail verbleibt. Beabsichtigt war auch, dass der Kunde informiert wird, wenn die von ihm angegebene E-Mail-Adresse nebst Anhang nicht zugestellt werden kann, wenn dessen Provider keine Transportverschlüsselung anbietet. Hierzu empfahl das ULD die Einrichtung eines Testversands, gegebenenfalls in Kombination mit der Bestätigungs-E-Mail zur Nutzung des Angebots, um die Fähigkeit zur Transportverschlüsselung zu gewährleisten.

Was ist zu tun?

Nachdrücklich empfohlen wird den öffentlichen Stellen die Lektüre der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“. Nicht nur für die Konzeption neuer, sondern auch für bereits etablierte Verfahren können die dort formulierten Vorgaben eine Hilfestellung bieten.

4.1.10 Prüfung eines kommunalen Rechenzentrums im Jahr 2019 – Mängelbehebung dauert an

Die Anforderungen an kommunale Rechenzentren werden auch aufgrund der zunehmenden Digitalisierung von Verwaltungsaufgaben immer komplexer. Insbesondere Datenschutz und Informationssicherheit müssen deshalb einen hohen Stellenwert erhalten, damit die Verarbeitungstätigkeiten in einem Rechenzentrum datenschutzkonform umgesetzt werden können. Bei einer datenschutzrechtlichen Überprüfung eines kommunalen Rechenzentrums im Frühjahr 2019 stellte das ULD jedoch fest, dass sowohl die Verantwortlichen des Rechenzentrums als auch eine Zahl von Kommunen als Träger des Rechenzentrums für die personenbezogene Datenverarbeitung keine Datenschutzkonformität nachweisen konnten.

Noch während der Prüfung musste das ULD aufgrund der gravierenden Mängel und Datenschutzverstöße eine Anweisung nach Art. 58 Abs. 2 Buchst. d DSGVO gegenüber den Verantwortlichen des Rechenzentrums aussprechen. Hierzu gehörten u. a. folgende Punkte:

- Die Kennwörter der Administrationskonten der Beschäftigten des Rechenzentrums waren zum Teil trivial und wurden schon seit mehreren Jahren nicht geändert. Teilweise wurden Kennwörter für Fachverfahren und technische Komponenten bei der Übernahme im Rahmen der Migration der Kommunen übernommen und seither nicht geändert. Vereinzelt wurden Kennwörter wie z. B. „Geheim“ oder „12345“ oder Kennwörter, die identisch mit der Benutzerkennung waren, festgestellt. Darüber hinaus wurde für das Standardadministrationskonto „Administrator“, das auf allen Windows-Systemen vorhanden ist und über Vollzugriffsrechte verfügt, dasselbe Kennwort verwendet.

- In der Benutzer- und Gruppenkontenverwaltung (Active Directory) wurden mehr als 70 Administrationsbenutzerkonten festgestellt, die über vollständige administrative Berechtigungen auf IT-Systeme des Rechenzentrums und der mit ihnen verarbeiteten personenbezogenen Daten der Kommunen verfügten. Einem Mitarbeiter eines externen Dienstleisters wurde sogar ein Konto als „Superadministrator“ eingerichtet. Ferner wurde festgestellt, dass ein ausgeschiedener Beschäftigter des Rechenzentrums als Administrator noch immer über Berechtigungen verfügte, sodass er jederzeit unbemerkt über externe Zugänge auf IT-Systeme des Rechenzentrums und auf Daten der Kommunen hätte zugreifen können.
- Zahlreiche vom Rechenzentrum beauftragte Dienstleister konnten über eingerichtete Zugänge von ihrem Standort aus auf IT-Systeme des Rechenzentrums und auf personenbezogene Daten der Kommunen unkontrolliert zugreifen. Über Log-Dateien wurde festgestellt, dass innerhalb einer Woche über diese Zugänge mehr als 100 Zugriffe auf IT-Systeme stattfanden.

Im weiteren Verlauf bemühten sich die Verantwortlichen des Rechenzentrums zwar, die eklatanten Mängel abzustellen, es wurden jedoch bei den nachfolgenden Prüfungsterminen weitere schwerwiegende Mängel festgestellt, sodass die Liste der Verstöße gegen die DSGVO immer länger wurde. Hierzu gehörten z. B.

- unzureichende Verträge nach den Anforderungen des Artikels 28 DSGVO zwischen Rechenzentrum und Kommunen,
- fehlende Nachweise über die Umsetzung technischer und organisatorischer Maßnahmen zum Schutze der personenbezogenen Daten gemäß der Artikel 5, 24 und 32 DSGVO,
- fehlende Zutrittskontrollmaßnahmen einschließlich einer nicht dokumentierten und nicht kontrollierten Schlüsselvergabe für Technikräume,
- nicht fachgerechte Installation von Hardwarekomponenten sowie eine nicht fachgerechte Verkabelung der einzelnen IT-Komponenten in Technikschränken,
- seit dem Jahr 2015 Einsatz von nicht aktualisierten Serverbetriebssystemen mit fehlenden Sicherheitspatches,
- nicht dokumentierte Firewall-Regeln der eingesetzten Firewall-Systeme,
- kein mandantenfähiges und segmentiertes Datenkommunikationsnetz zwischen den einzelnen Kommunen und dem Rechenzentrum,
- keine Protokollierung administrativer Aktivitäten der Beschäftigten des Rechenzentrums und ihrer beauftragten Dienstleister sowie
- ein fehlerhaftes Berechtigungsmanagement mit über 5.000 Benutzer- und Gruppenkonten, die aufgrund ihrer komplexen Strukturen nicht mehr vollständig prüffähig waren.

Nach Abschluss der Prüfung bekundeten die Verantwortlichen über ihren mit der Sache beauftragten Rechtsanwalt gegenüber dem ULD, die Mängel zeitnah abzustellen. Darüber hinaus wurde das ULD in Wochenberichten über Pläne und Aktivitäten der Verantwortlichen des Rechenzentrums informiert.

Nachdem eineinhalb Jahre vergangen waren und die Berichte der Verantwortlichen keinen zufriedenstellenden Umsetzungsstand erkennen ließen, kündigte sich das ULD bei den Verantwortlichen des Rechenzentrums im Herbst 2020 mit einer Nachprüfung an. Bei dieser Prüfung wurde festgestellt, dass noch immer viele schwerwiegende Mängel und mithin Verstöße gegen die DSGVO vorlagen. Die dem ULD mitgeteilten geplanten Maßnahmen waren größtenteils nicht umgesetzt worden. Eine zum Jahresende vom Rechenzentrum beim ULD beauftragte Auditierung des Umsetzungsstands der Datenschutzmaßnahmen wurde von den Verantwortlichen des Rechenzentrums demzufolge abgesagt.

Im Ergebnis ist festzustellen, dass die Verantwortlichen seit Jahren keine Datenschutzkonformität für die Datenverarbeitung im Rechenzentrum gewährleisten und infolgedessen die Vorschriften der DSGVO nicht vollständig einhalten. Sonderbar ist auch, dass sie nach Erhalt des Prüfbescheids des ULD bei dem Verwaltungsgericht Schleswig-Holstein Klage erhoben haben.

Bußgelder können gegenüber öffentlichen Stellen nicht verhängt werden.

Was ist zu tun?

Die Verantwortlichen des Rechenzentrums sind aufgefordert, die schwerwiegenden Datenschutzmängel dringend abzustellen. Solange die Verantwortlichen des Rechenzentrums keine Datenschutzkonformität nachweisen können, sind die Kommunen in der Pflicht, ihre Datenverarbeitung im eigenen Hause datenschutzkonform zu gestalten oder für ihre Verarbeitungstätigkeiten ein Rechenzentrum zu beauftragen, das die Anforderungen der DSGVO erfüllt.

4.1.11 Gemeldete Datenpanne: Schadsoftware in der Kläranlage

Ein Versorgungsbetrieb meldete fristgerecht eine Verletzung des Schutzes personenbezogener Daten nach Artikel 33 DSGVO. Ein Virus hatte die Steuerung des Reinigungsprozesses beeinträchtigt. In diesem Zusammenhang war es den Mitarbeiterinnen und Mitarbeitern nur noch möglich, die Kläranlage manuell weiterzubetreiben. Durch den Virusbefall waren auch die Zugangsdaten der Mitarbeitenden zur Steuerungsanlage betroffen.

Im Zuge der Überprüfung analysierte der Versorgungsbetrieb den bestehenden Virenschutz, den Systemzugang und weitere getroffene technisch-organisatorische Maßnahmen. Befallene Rechner wurden umgehend vom Netz getrennt. Die mitgeteilten Maßnahmen waren angemessen. Insbesondere informierte der Versorgungsbetrieb unverzüglich alle Mitarbeiterinnen und Mitarbeiter über den Vorfall.

Art. 4 Nr. 12 DSGVO

Im Sinne der DSGVO bezeichnet der Ausdruck „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Was ist zu tun?

Eine Meldepflicht gegenüber der Aufsichtsbehörde besteht auch dann, wenn kein vorsätzliches oder fahrlässiges Verhalten des Verantwortlichen belegt ist. Ausgangspunkt ist das Bestehen einer Verletzung des Schutzes personenbezogener Daten unter Berücksichtigung eines Risikos für die Rechte und Freiheiten natürlicher Personen.

4.1.12 Gemeldete Datenpanne: Einbruch in Büroräume

Eine öffentliche Stelle unterrichtete das ULD fristgerecht über einen Einbruch in Büroräume. Die Täter beschädigten dabei auch Schränke, in denen Personalakten lagerten. Im Rahmen der Überprüfung, ob einzelne Personalakten oder Bestandteile hierin fehlen, konnte kein Verlust festgestellt werden.

Auch papiergebundene Personalakten zählen zu den personenbezogenen Daten, deren Schutz in der DSGVO geregelt ist. Die Personalakten führte die öffentliche Stelle damit in Form einer nicht automatisierten Verarbeitung unter Nutzung eines Dateisystems.

Die getroffenen technisch-organisatorischen Sicherungsmaßnahmen waren angemessen und gaben keinen Anlass zur Beanstandung.

Da eine unbefugte Kenntnisnahme von Personalakten durch die Täter nicht ausgeschlossen werden konnte, unterrichtete die öffentliche Stelle auch sämtliche Mitarbeiterinnen und Mitarbeiter über den Einbruch und das in diesem Zusammenhang ermittelte Risiko. Die Unterrichtung war aus Sicht des ULD sachgerecht.

Art. 4 Nr. 6 DSGVO

Im Sinne der DSGVO bezeichnet der Ausdruck „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

Was ist zu tun?

Eine Benachrichtigungspflicht gegenüber den betroffenen Personen besteht neben der Meldepflicht gegenüber der Aufsichtsbehörde dann, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

4.2 Polizei und Verfassungsschutz

4.2.1 Neues Polizeirecht für Schleswig-Holstein

Der Landtag hat im Berichtszeitraum eine Änderung des Polizeirechts beraten. Ziel der Änderung ist u. a. die Umsetzung der EU-Richtlinie 2016/680 zum Datenschutz in der Strafverfolgung und des Urteils des Bundesverfassungsgerichts zum BKA-Gesetz. Gegenüber dem Landtag hatten wir Gelegenheit, zu dem Entwurf Stellung zu nehmen. Wir haben in unserer Stellungnahme zahlreiche Kritikpunkte wiederholt, die wir schon gegenüber dem Innenministerium vorgetragen hatten (38. TB, Tz. 4.2.1). Einige Änderungen hatte das Innenministerium aufgrund unserer Stellungnahme vorgenommen, aber in vielen Punkten war der Entwurf bei seiner Vorlage an den Landtag unverändert.

Das Gesetz enthält eine Reihe von Verbesserungen für den Datenschutz. Allerdings wiegen diese den Zuwachs an Befugnissen für die Erhebung und Verarbeitung personenbezogener Daten nicht auf, die mit dem Gesetz eingeführt werden. Zu den vorgesehenen Neuerungen gehören eingriffsintensive Maßnahmen wie z. B. GPS-Tracking, der Einsatz verdeckter Ermittler oder die Durchführung von verdachtsunabhängigen Kontrollen in Verkehrsmitteln und auf Verkehrswegen.

Kritik haben wir insbesondere zu folgenden Regelungen geäußert:

- zu der Einführung einer Befugnis zur anlasslosen Identitätsfeststellung in Verkehrsmitteln und auf Durchgangsstraßen für den grenzüberschreitenden Verkehr,
- zu dem Einsatz von Bodycams auch auf Wohngrundstücken,
- zu der neu eingeführten Definition der dringenden Gefahr und
- zu der Absenkung des Schutzes des Kernbereichs privater Lebensgestaltung bei der Wohnraumüberwachung.

Unsere Stellungnahme ist hier abrufbar:

http://www.landtag.ltsh.de/infothek/wahl19/umdrucke/04400/umdruck-19-04443.pdf

Kurzlink: *https://uldsh.de/tb39-4-21*

4.2.2 Stichprobenkontrolle bei Telekommunikationsüberwachung (TKÜ)

Das verdeckte Abhören von Telefongesprächen ist ein schwerer Eingriff in die Persönlichkeitsrechte der betroffenen Personen. Regelmäßig sind auch unbeteiligte Dritte davon berührt, ohne dies zu wissen. Das Verfahren ist technisch aufwendig, und neben den Providern und der Polizei sind in Strafverfahren auch die Staatsanwaltschaften und Gerichte beteiligt.

Für das Vertrauen der Bevölkerung in die Rechtmäßigkeit verdeckter Maßnahmen ist die Überzeugung entscheidend, dass diese nach rechtsstaatlichen Prinzipien durchgeführt werden. Es liegt in der Natur der Sache, dass verdeckte Maßnahmen für Betroffene sowie Außenstehende intransparent sind. Häufig reichen deshalb bereits leichte Zweifel aus, um das Vertrauen in die rechtmäßige Anwendung dieser Instrumente zu untergraben.

Hier leistet die unabhängige datenschutzrechtliche Kontrolle einen wichtigen Beitrag. Dies hat auch das Bundesverfassungsgericht beispielsweise in seinem Urteil zum BKA-Gesetz betont. Die unabhängige Kontrolle mildert die Folgen der Intransparenz, kann das Vertrauen der Öffentlichkeit in die rechtmäßige Anwendung dieser Instrumente stärken und trägt dazu bei, Prozesse und Verfahrensweisen zu verbessern.

Aufgrund mehrerer Eingaben von Bürgerinnen und Bürgern, die befürchteten, unrechtmäßig abgehört worden zu sein, haben wir bereits Mitte 2018 begonnen, Telekommunikationsüberwachungsmaßnahmen (TKÜ-Maßnahmen) bei der Landespolizei stichprobenweise zu kontrollieren. Zu der Stichprobe gehörten 20 Vorgänge, die aus der TKÜ-Anlage der Polizei ausgewählt wurden, mit insgesamt 126 einzelnen Maßnahmen. Darüber hinaus wurden die 20 ältesten Vorgänge herangezogen, zu denen noch Aufnahmen existierten.

Für alle 126 Einzelmaßnahmen wurde vor Ort geprüft, ob die erforderlichen Gerichtsbeschlüsse vorliegen. Darüber hinaus wurden in der Folge bei den betroffenen Staatsanwaltschaften die Punkte der Löschung der Daten und der Information der Betroffenen geprüft.

Das Landeskriminalamt (LKA) konnte im Rahmen einer Vor-Ort-Prüfung für alle 126 Maßnahmen der Stichprobe ad hoc die entsprechenden Gerichtsbeschlüsse vorlegen. Das ULD wurde in seiner Prüfung unterstützt, und offene Fragen wurden jeweils engagiert und zeitnah beantwortet. Die Dokumentation war vollständig und übersichtlich abgelegt.

Auffälligkeiten wurden in zwei Bereichen vorgefunden: der Löschung von Altaufnahmen sowie der Benachrichtigung Betroffener.

1. Löschung von Altdaten: Im LKA existierten noch alte Aufnahmen, die bis in die 90er-Jahre zurückreichten. Ursache dafür waren Mängel in der Zusammenarbeit zwischen der Polizei und den Staatsanwaltschaften. Über die Löschung von TKÜ-Aufnahmen in einem Strafverfahren entscheidet grundsätzlich die Staatsanwaltschaft. Das LKA wird dann angewiesen, die Löschung durchzuführen und zu bestätigen. Dies wurde offensichtlich in vielen Fällen schlicht vergessen. Nachfragen vonseiten der Polizei gab es ebenfalls nicht.

Seit dem Beginn der Prüfung haben Polizei und Staatsanwaltschaften jedoch verstärkt zusammengearbeitet, um Datenbestände zu löschen, die nicht mehr benötigt werden. So konnten seit Beginn der Prüfung gemäß einer Schätzung des LKA Daten zu ca. 8.500 (+/- 250) Leitungen in ca. 1.000 (+/- 100) Verfahren gelöscht werden.

Begriffe

„Verfahren“ sind Ermittlungsverfahren, zu denen sich einzelne **„TKÜ-Maßnahmen“** zu bestimmten Personen oder Kommunikationsmitteln ergeben können. Dabei werden die anfallenden Daten für einzelne **„Leitungen“** getrennt gespeichert, die auch dieselbe Rufnummer betreffen können, wenn diese etwa im In- oder Ausland oder unabhängig voneinander für verschiedene Verfahren überwacht wird.

2. Benachrichtigung Betroffener: Weiteres Verbesserungspotenzial besteht bei der Benachrichtigung der von der Telekommunikationsüberwachung betroffenen Personen. Die Strafprozessordnung sieht vor, dass die Beteiligten an der überwachten Kommunikation benachrichtigt werden sollen, sobald der Untersuchungszweck nicht mehr gefährdet ist. In diesem Zusammenhang soll auch

auf die Möglichkeit des nachträglichen Rechtsschutzes sowie die entsprechenden Fristen hingewiesen werden. Das gilt grundsätzlich auch für die Kommunikationspartner einer überwachten Person. Unter bestimmten Umständen kann davon abgesehen werden: z. B. wenn der Kommunikationspartner von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass er kein Interesse an einer Benachrichtigung hat. Oder falls der Aufwand für die Ermittlung des Kommunikationspartners besonders hoch und dies sehr eingriffsintensiv wäre. Eine Benachrichtigung darf jedoch nicht einfach pauschal deswegen unterbleiben, weil dies mit einem zusätzlichen Aufwand verbunden ist. Die für die Überwachung zuständige Behörde muss dokumentieren, für welche Variante sie sich jeweils entscheidet, und dabei darlegen, warum die Voraussetzungen dafür vorliegen.

In den in Augenschein genommenen Akten sind derartige Dokumentationen (bis auf eine Ausnahme) zur (Nicht-)Benachrichtigung der Betroffenen nicht gefunden worden. Betroffene werden häufig im Rahmen des Gerichtsverfahrens durch die Akteneinsicht ihrer Verteidiger auf die TKÜ-Maßnahmen aufmerksam. Dokumentierte Entscheidungen bezüglich der Benachrichtigung der einzelnen Kommunikationspartner waren ebenfalls nicht in den Akten enthalten.

Lösungsansatz: Die vorgefundenen Mängel liegen häufig in der Art begründet, wie die Akten geführt werden. Verfahren, bei denen TKÜ-Maßnahmen zum Einsatz kommen, können mitunter viele Jahre laufen, mehrere Beschuldigte umfassen, und es können jeweils viele Kommunikationsmittel eine Rolle spielen. Hierbei darf man nicht den Überblick verlieren. Es gibt zwar teilweise TKÜ-Sonderbände, in den geprüften Akten enthielten diese zumeist aber nur inhaltliche Auszüge aus einzelnen Überwachungsmaßnahmen. Es war kaum möglich, in den Aktenbergen die relevanten Dokumente zu finden.

Die Situation könnte beispielsweise dadurch verbessert werden, dass man in den TKÜ-Sonderbänden alle TKÜ-relevanten Informationen zentral sammelt. Dazu gehören Unterlagen wie die gerichtlichen Anordnungen, eine Übersicht der an der überwachten Kommunikation beteiligten Personen, eine Übersicht der überwachten Leitungen bzw. Kommunikationsmittel sowie die Dokumentation von Löschverfügungen und von erteilten oder nicht notwendigen Benachrichtigungen.

Mit einer auf diese Weise verbesserten Übersichtlichkeit könnte auch einfacher sichergestellt werden, dass die Rechte betroffener Personen – z. B. durch fristgerechte Löschung oder Benachrichtigung – gewahrt werden. Außerdem kann dies das Vertrauen in verdeckte Maßnahmen stärken, da so eine effektive unabhängige Kontrolle unterstützt wird.

Was ist zu tun?

Die Dokumentation bezüglich der Benachrichtigung betroffener Personen sowie die Kommunikation der Staatsanwaltschaften mit dem LKA bezüglich der fristgerechten Löschung von Aufnahmen müssen verbessert werden. Um den Überblick zu behalten, Löschfristen und Benachrichtigungsverpflichtungen nicht zu übersehen sowie eine unabhängige Kontrolle zu erleichtern, könnten alle TKÜ-relevanten Dokumente und Vermerke in einem Sonderband gesammelt werden.

4.2.3 Protokollierung von Abfragen aus polizeilichen Systemen

Immer häufiger liest man in letzter Zeit davon, dass offenbar personenbezogene Daten aus polizeilichen Systemen zweckentfremdet genutzt werden. Besondere Aufmerksamkeit bekommt das Thema rund um die Aktivitäten des sogenannten NSU 2.0. Dies ist ein besonders gravierender Missbrauch, der in unserer Aufsichtspraxis glücklicherweise keine Rolle gespielt hat. Missbräuchliche Abrufe beschäftigen uns dagegen seit langer Zeit. Meist steckt die persönliche Neugier der Polizeibeamtinnen und -beamten dahinter.

Unzulässige Abfragen fallen in der Regel nur auf, wenn es einen konkreten Verdacht gibt. Selbst dann ist es häufig mühsam oder gar nicht möglich, einen Verstoß nachzuweisen. Abfragen werden grundsätzlich protokolliert und lassen sich dem Nutzerkonto einer bestimmten Beamtin oder eines bestimmten Beamten zuordnen. Liegt eine Abfrage länger zurück und soll dann auf Nachfrage begründet werden, ist es bei der Vielzahl an Abfragen oft schwierig, sich zu erinnern, warum eine zurückliegende Abfrage (rechtmäßig) getätigt wurde.

Diese Situation ist in mehrfacher Hinsicht problematisch. Einerseits haben es diejenigen Polizistinnen und Polizisten, die sich an die Regeln halten, häufig schwer, die Rechtmäßigkeit ihrer Abfrage nachträglich zu belegen. Gibt es bereits einen Verdacht auf Missbrauch, geraten sie in einen Rechtfertigungszwang. Andererseits fällt eine missbräuchliche Nutzung selten auf und kann manchmal durch Schutzbehauptungen verschleiert werden. Personen, die von solchen Abfragen betroffen sind, fühlen sich dadurch wehrlos und ausgeliefert. Und wie die öffentliche Diskussion zeigt, sind diese Umstände auch geeignet, das Vertrauen in den Umgang mit polizeilichen Daten sowie das Ansehen der Polizei im Allgemeinen zu schädigen. Doch die derzeitigen Inhalte der Protokolldateien sind nicht dazu geeignet, um effektive verdachtsunabhängige Kontrollen durch Datenschutzaufsichtsbehörden oder behördliche Datenschutzbeauftragte zu bewerkstelligen.

Mit der Umsetzung der EU-Richtlinie 2016/680 in nationales Recht hat der Landesgesetzgeber die rechtliche Grundlage für eine Verbesserung der Situation gelegt. § 52 Abs. 2 LDSG legt nun erstmals fest, dass die Protokolle über Abfragen und Offenlegungen es ermöglichen müssen, **die Begründung**, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich **die Identität der Person**, die die personenbezogenen Daten abgefragt oder offengelegt hat, sowie die **Identität des Empfängers** der Daten festzustellen.

Auf dieser Grundlage wird es zukünftig möglich sein, Missbrauch effektiver zu bekämpfen, aber im Bedarfsfall auch die rechtmäßige Verwendung von personenbezogenen Daten nachzuweisen. Um dies zu bewerkstelligen, sind umfangreiche Anpassungen der polizeilichen IT-Systeme erforderlich. Dabei sind noch viele Fragen offen. Dazu gehört beispielsweise, wie die Identität der abfragenden Person sowie des Empfängers zweifelsfrei festgestellt werden soll (Authentifizierung). Auch ist noch unklar, welche Voraussetzungen und Merkmale eine Begründung erfüllen muss, um die Rechtmäßigkeit einer Abfrage effektiv überprüfen zu können. Dabei ist nicht nur die konsequente Erfassung der notwendigen Informationen in den bestehenden Protokollen von Bedeutung. Durch die Einführung automatisierter Plausibilitätschecks sowie technisch auswertbarer Protokollformate könnte man die anstehenden Änderungen auch nutzen, um anlasslose, unabhängige Kontrollen trotz begrenzter personeller Ressourcen deutlich zu erleichtern.

Das Gesetz sieht für die Anpassung bestehender IT-Systeme eine Übergangsfrist bis zum 06.05.2023 vor. Die Praxis zeigt, dass diese Anpassungen dringend nötig sind.

Was ist zu tun?

Es sollte zeitnah für die jeweils betroffenen IT-Systeme ein Lastenheft für die konkrete Umsetzung der neuen Regelungen zur Protokollierung erstellt werden. Entscheidend ist dabei, dass die Anforderungen an eine effektive Kontrolle der Protokolldaten ebenfalls Berücksichtigung finden. Die Übergangszeit bis 2023 muss nicht ausgeschöpft werden – je schneller der aktuelle unbefriedigende Zustand behoben wird, desto besser.

4.2.4 Kein Zugriff auf Corona-Kontaktdaten für die Polizei!

Im Zuge der Erhebung von Kontaktdaten von Gästen in der Gastronomie und in anderen Freizeiteinrichtungen stellte sich immer wieder die Frage, ob auch die Polizei diese Daten für strafrechtliche Ermittlungen oder für Gefahrenabwehrmaßnahmen erhalten darf. Dies hat der Bundesgesetzgeber nun mit einem klaren „Nein“ beantwortet.

Seit der Einführung der Pflicht zur Erhebung der Kontaktdaten enthielt die Corona-Bekämpfungsverordnung des Landes eine Zweckbeschränkung dieser Daten. Die Gastwirte und andere Einrichtungen durften diese Daten nur für die Nachverfolgung von Infektionsketten an die Gesundheitsbehörden herausgeben. Für andere Zwecke durften die Daten nicht genutzt werden.

Diese Zweckbeschränkung in einer Rechtsverordnung eines Landes war jedoch nicht geeignet, Anforderungen vonseiten Dritter standzuhalten, die auf einer gesetzlichen Grundlage die Herausgabe verlangen können, wie z. B. eine Beschlagnahme durch Strafverfolgungsbehörden.

Durch eine Änderung im Infektionsschutzgesetz hat nun der Bundesgesetzgeber eine klare und abschließende Zweckbeschränkung für solche Kontaktdaten geregelt.

Damit ist nun sichergestellt, dass die Kontaktdaten ausschließlich für die Zwecke der Nachverfolgung von Kontaktpersonen einer mit dem Coronavirus infizierten Person verwendet werden dürfen. Für Zwecke der Strafverfolgung oder Gefahrenabwehr dürfen sie nicht verwendet werden.

§ 28a Abs. 4 Infektionsschutzgesetz

Im Rahmen der Kontaktdatenerhebung nach Absatz 1 Nummer 17 dürfen von den Verantwortlichen nur personenbezogene Angaben sowie Angaben zum Zeitraum und zum Ort des Aufenthaltes erhoben und verarbeitet werden, soweit dies zur Nachverfolgung von Kontaktpersonen zwingend notwendig ist. Die Verantwortlichen haben sicherzustellen, dass eine Kenntnisnahme der erfassten Daten durch Unbefugte ausgeschlossen ist. **Die Daten dürfen nicht zu einem anderen Zweck als der Aushändigung auf Anforderung an die nach Landesrecht für die Erhebung der Daten zuständigen Stellen verwendet werden** und sind vier Wochen nach Erhebung zu löschen. Die zuständigen Stellen nach Satz 3 sind berechtigt, die erhobenen Daten anzufordern, soweit dies zur Kontaktnachverfolgung nach § 25 Absatz 1 erforderlich ist. Die Verantwortlichen nach Satz 1 sind in diesen Fällen verpflichtet, den zuständigen Stellen nach Satz 3 die erhobenen Daten zu übermitteln. Eine Weitergabe der übermittelten Daten durch die zuständigen Stellen nach Satz 3 oder eine Weiterverwendung durch diese zu anderen Zwecken als der Kontaktnachverfolgung ist ausgeschlossen. Die den zuständigen Stellen nach Satz 3 übermittelten Daten sind von diesen unverzüglich irreversibel zu löschen, sobald die Daten für die Kontaktnachverfolgung nicht mehr benötigt werden.

Was ist zu tun?

Die enge Zweckbestimmung der Kontaktdaten ist zu beachten. Sie dürfen durch die erhebenden Stellen und die Gesundheitsbehörden nur für den Zweck der Kontaktnachverfolgung genutzt werden. Für andere Zwecke und für die Nutzung durch andere Stellen stehen sie nicht zur Verfügung.

4.3 Justiz

4.3.1 Änderung des Datenschutzrechts für den Justizvollzug

Die Landesregierung hat im Berichtszeitraum einen Entwurf für ein Justizvollzugsmodernisierungsgesetz vorgelegt. Darin ist auch eine umfangreiche Änderung des Justizvollzugsdatenschutzgesetzes vorgesehen. Hier soll die EU-Richtlinie 2016/680 zum Datenschutz in der Strafverfolgung umgesetzt werden.

Der Gesetzentwurf muss an einigen Stellen geändert werden, um mit der EU-Richtlinie in Einklang gebracht zu werden:

- Es müssen Begrifflichkeiten so gewählt bzw. definiert werden, dass sie dem europäischen Datenschutzrecht entsprechen. Dies betrifft die Definition der „Anonymisierung“ sowie die Begriffe der „Erhebung“, „Speicherung“ und „Nutzung“. Letztere müssen durch den europarechtlichen Begriff der „Verarbeitung“ ersetzt werden, um Regelungslücken zu vermeiden.
- Für die Verarbeitung besonderer Arten personenbezogener Daten fehlt es an den nach der EU-Richtlinie erforderlichen geeigneten Garantien zum Schutz der Rechte und Freiheiten der betroffenen Personen.
- Es fehlt eine Regelung zur Umsetzung der Vorgaben der EU-Richtlinie zum Datenschutz durch Technikgestaltung (Data Protection by Design).
- Dort, wo die EU-Richtlinie von „Risiken“ für die Rechte und Freiheiten betroffener Personen spricht, verwendet der Gesetzentwurf den Begriff „Gefahren“. Dies ist irreführend, da nach der EU-Richtlinie keine Gefahren im Sinne des deutschen Gefahrenabwehrrechts gemeint sind. Es sollte daher der Begriff der „Risiken“ verwendet werden.
- Bei der Protokollierung von Abfragen aus Datenbanken sollte entsprechend den Vorgaben der EU-Richtlinie auch der Abfragegrund protokolliert werden (siehe auch Tz. 4.2.3).
- Die Ausnahmen vom Auskunftsanspruch der betroffenen Personen sind zu weit gefasst.
- Eine europarechtlich bedenkliche Regelung enthält der Entwurf für die Einsicht in Gesundheitsakten. Die hier getroffene Regelung widerspricht zum Teil dem Auskunftsanspruch nach der DSGVO, der allerdings auf die hier geregelte medizinische Behandlung unmittelbar anwendbar sein dürfte.

Diese und weitere Punkte hatten wir bereits gegenüber dem Justizministerium im Rahmen seiner Beteiligung geäußert. Der Gesetzentwurf wurde in diesen Punkten leider weitgehend unverändert in den Landtag eingebracht. Im Gesetzgebungsverfahren haben wir schriftlich und in der mündlichen Anhörung erneut auf den Änderungsbedarf hingewiesen.

Unsere Stellungnahme ist hier abrufbar:

http://www.landtag.ltsh.de/infothek/wahl19/umdrucke/04700/umdruck-19-04779.pdf

Kurzlink: *https://uldsh.de/tb39-4-31*

Was ist zu tun?

Für eine europarechtskonforme Umsetzung der EU-Richtlinie muss der Gesetzentwurf zur Änderung des Justizvollzugsdatenschutzgesetzes geändert werden. Auch darüber hinaus besteht in einigen Punkten Verbesserungsbedarf.

4.3.2 Erhebung von Besucherdaten in den Gerichten als Coronamaßnahme

Die Gerichte stehen wie viele andere öffentliche Einrichtungen vor der Herausforderung, ihren Betrieb auch in Zeiten der Coronapandemie aufrechtzuerhalten und gleichzeitig den Infektionsschutz für Besucherinnen und Besucher sowie für die Mitarbeitenden des Gerichts zu wahren. Nach anfänglichen Schwierigkeiten hat das Justizministerium in enger Abstimmung mit uns eine tragfähige Lösung entwickelt.

Nach der aktuellen Fassung der Corona-Bekämpfungsverordnung des Landes sind die Gerichte und Staatsanwaltschaften verpflichtet, von ihren Besucherinnen und Besuchern Kontaktdaten zu erheben. Damit ist im Infektionsfall die Möglichkeit einer Kontaktnachverfolgung durch die Gesundheitsämter gewährleistet.

Auf weiter gehende Datenerhebungen verzichtet die Justiz. Besucherinnen und Besucher erhalten rechtzeitig vor ihrem Termin Informationen über die Maßnahmen zum Coronaschutz. Darin werden sie aufgefordert, nicht zum Termin zu erscheinen, wenn sie Kontakt zu Infizierten hatten, sich in Quarantäne befinden oder bestimmte Krankheitssymptome haben. Ein früher verwendeter Fragebogen, in dem alle Besucherinnen und Besucher Angaben zu Krankheitssymptomen wie Fieber, Husten, Kopfschmerzen, Bindehautentzündung, Bauchschmerzen oder Gewichtsverlust machen mussten, wurde nach unserem Einschreiten verworfen. Gegen diesen Fragebogen haben wir zahlreiche Beschwerden, vor allem von Rechtsanwältinnen und Rechtsanwälten und von Behördenvertreterinnen und -vertretern, erhalten. Sie haben befürchtet, dass sie gezwungen werden, vorhandene Erkrankungen – etwa eine Pollenallergie – zu offenbaren, um ihre vorhandenen Symptome zu erklären und Einlass zum Gericht zu erhalten. Die im Fragebogen aufgeführten Symptome waren derart weit gefasst, dass sie nicht nur auf COVID-19-Erkrankungen hindeuteten, sondern praktisch mit jeder Erkrankung oder gesundheitlichen Beeinträchtigung einhergehen könnten. Bei wahrheitsgemäßer Beantwortung des Fragebogens hätten so zahlreiche nicht infizierte Besucherinnen und Besucher befürchten müssen, erst nach Erläuterung ihres Gesundheitszustands oder gar nicht Einlass zum Gerichtsgebäude zu erhalten. Angesichts der erheblichen Sensibilität der Daten und des jedenfalls für Rechtsanwälte berufsregelnden Charakters war diese Datenerhebung unverhältnismäßig.

4.3.3 Berichte über politisch relevante Strafverfahren

Im Berichtszeitraum erhielten wir Beschwerden zu den Berichten, die die Staatsanwaltschaft in einem Ermittlungsverfahren wegen des Verdachts des Verrats von Dienstgeheimnissen an das Justizministerium erstattet hat. Diese Berichte wurden nach der **Anordnung über Berichtspflichten in Strafsachen (BeStra)** erstattet. Danach ist dem Justizministerium über Strafverfahren zu berichten, wenn zu erwarten ist, dass das Verfahren weitere Kreise, insbesondere parlamentarische Gremien, beschäftigten wird. In diesem Fall gab das Justizministerium die Berichte an den Ministerpräsidenten weiter. Dies führte im April 2020 zum Rücktritt des Innenministers.

Bei unserer Prüfung konnten wir letztlich keine Verstöße gegen datenschutzrechtliche Vorschriften feststellen. Die Weitergabe von personenbezogenen Daten im Rahmen von BeStra-Berichten kann zulässig sein, wenn dies **für die Zwecke der Fachaufsicht im Einzelfall erforderlich** ist (siehe 35. TB, Tz. 4.3.8). Die Fallgruppen, in denen Informationen für die Wahrnehmung der Fachaufsicht erforderlich sind, sind in der BeStra konkretisiert. Dass deren Voraussetzungen hier grundsätzlich vorlagen, lag auf der Hand. Denn **Gremien des Landtages** hatten sich bereits mit der Angelegenheit befasst. Die Berichte bezogen sich auf die von der Staatsanwaltschaft durchgeführten Ermittlungen. Die Ermittlungen selbst haben wir nicht geprüft.

4.3.4 Ersatzzustellung durch Gerichtsvollzieher nur in verschlossenem Umschlag

Im Berichtszeitraum wandte sich ein Bürger an uns und beschwerte sich über einen Gerichtsvollzieher, der einen Pfändungs- und Überweisungsbeschluss an seinen Arbeitgeber zugestellt hatte. Da der Gerichtsvollzieher bei der Zustellung weder die Geschäftsführung noch Mitarbeitende der Personalabteilung angetroffen hatte, übergab er den Beschluss einem Mitarbeiter, der nicht mit der Angelegenheit befasst war. Insoweit ist das Handeln des Gerichtsvollziehers nicht zu beanstanden. Eine Ersatzzustellung ist im Fall der Abwesenheit der Unternehmensleitung an jede beim Unternehmen beschäftigte Person möglich.

Allerdings hatte der Gerichtsvollzieher es **versäumt, den Beschluss in einem Umschlag zu verschließen**. Dem Mitarbeiter, der nun den Beschluss erhalten hatte, war es daher möglich, den Beschluss vollständig zur Kenntnis zu nehmen. Hierin sah der Beschwerdeführer zu Recht eine Verletzung des Datenschutzes. Die Geschäftsanweisung für Gerichtsvollzieher schreibt ausdrücklich vor, dass der Gerichtsvollzieher das zu übergebende Schriftstück bei jeder Zustellung an einen Ersatzempfänger in einem Umschlag verschließen muss. Das Schriftstück ist danach so zu verschließen, dass es ohne Öffnung nicht eingesehen werden kann.

Wir haben aufgrund des Verstoßes gegenüber dem Gerichtsvollzieher eine Verwarnung ausgesprochen.

Was ist zu tun?

Die meisten Beschwerden über Gerichtsvollzieher betreffen die Zustellung von Schriftstücken. Hierbei kann vieles schiefgehen. Die Geschäftsanweisung für Gerichtsvollzieher (GVGA) regelt detailliert, was Gerichtsvollzieher zu beachten haben – nicht nur bei der Zustellung. Sie berücksichtigt auch den notwendigen Schutz personenbezogener Daten. Wer die Vorgaben der GVGA einhält, beachtet damit auch das Datenschutzrecht.

4.3.5 Beschwerden über justizielle Tätigkeiten gehen ins Leere

Auch im Berichtszeitraum haben uns wie jedes Jahr viele Beschwerden über justizielle Tätigkeiten der Gerichte erreicht. Bei den Beschwerden ging es z. B. darum, dass und in welchem Umfang Daten aus dem Gerichtsverfahren an Sachverständige für die Erstellung von Gutachten weitergegeben werden, welche Informationen das Gericht von den Parteien als Beweis für ihr Vorbringen in der jeweiligen Sache verlangt oder welche Informationen aus dem Gerichtsverfahren in der Begründung der Entscheidung genannt und so den Beteiligten des Verfahrens zur Kenntnis gegeben werden.

Diese justiziellen Verarbeitungen sind unserer Kontrolle entzogen. Bereits der Grundsatz der Gewaltenteilung verbietet eine Kontrolle der rechtsprechenden Gewalt durch eine Exekutivbehörde.

Den Beschwerdeführerinnen und Beschwerdeführern ist dies im Grundsatz zwar regelmäßig vermittelbar. Mit großem Unverständnis reagieren sie hingegen, wenn wir auf ihre Nachfrage, an wen sie sich stattdessen wenden können, keine Antwort geben können. Ihnen ist bekannt, dass das Datenschutzrecht für sämtliche Verarbeitungen der Justiz gilt und somit ihre Rechte als betroffene Personen genauso gegenüber den Gerichten gelten. Dass aber ihr Beschwerderecht bei einer unabhängigen Stelle für justizielle Tätigkeiten der Gerichte ins Leere läuft, hinterlässt bei ihnen häufig den Eindruck, als müssten die Gerichte sich an die gesetzlichen Vorgaben nicht halten und als könnten die Betroffenen gegen etwaige Rechtsverletzungen nichts ausrichten.

Ein Blick in die Datenschutz-Grundverordnung zeigt, dass die Beschwerdeführer mit ihrem Rechtsempfinden nicht ganz falsch liegen. Zwar ist die Kontrolle justizieller Tätigkeiten durch die Aufsichtsbehörde ausdrücklich ausgenommen. Dies soll jedoch nicht bedeuten, dass eine unabhängige Kontrolle nicht stattfindet. Die DSGVO betrachtet in ihrem Erwägungsgrund 20 diese Konstellation und sieht justizeigene Stellen als Aufsicht für Datenverarbeitungsvorgänge im Rahmen justizieller Tätigkeiten vor.

In der Praxis nehmen sich häufig die Präsidentinnen und Präsidenten oder Direktorinnen und Direktoren der Gerichte solcher Beschwerden an, und oftmals kann hier auch eine für die Beschwerdeführerinnen und Beschwerdeführer akzeptable Lösung gefunden werden. Dies erfolgt im Wege der Dienstaufsicht. Die unabhängige Datenschutzaufsicht im Sinne des Erwägungsgrunds 20 der DSGVO ist den Leitungen der Gerichte hingegen nicht zugewiesen.

Dass ein Bedarf für solche unabhängigen Kontrollstellen besteht, zeigen nicht nur die Beschwerden, die uns erreichen. Auch konkrete Beratungsanfragen der Verantwortlichen im Bereich ihrer justiziellen Tätigkeiten konnten wir nicht beantworten. Denn auch Schulungen oder Beratungen sowie über den Einzelfall hinausgehende Kontrollen sind in diesem Bereich zurzeit nicht möglich: Weder wir als Datenschutzaufsichtsbehörde noch die Datenschutzbeauftragten der Gerichte haben nach der DSGVO Aufgaben und Befugnisse im Bereich der justiziellen Tätigkeit.

Das Beispiel der gesetzgebenden Gewalt zeigt seit vielen Jahren schon, dass eine Kontrolle innerhalb der eigenen Gewalt möglich ist. Hier hat sich das Datenschutzgremium als Kontrollstelle des Landtages bewährt (Tz. 3.1). Dieses Modell könnte auch für die Justiz ein Vorbild sein.

Erwägungsgrund 20 der DSGVO

Diese Verordnung gilt zwar u. a. für die Tätigkeiten der Gerichte und anderer Justizbehörden, doch könnte im Unionsrecht oder im Recht der Mitgliedstaaten festgelegt werden, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und andere Justizbehörden im Einzelnen auszusehen haben. Damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt, sollten die Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein. **Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollten besondere Stellen im Justizsystem des Mitgliedstaats betraut werden können, die insbesondere die Einhaltung der Vorschriften dieser Verordnung sicherstellen, Richter und Staatsanwälte besser für ihre Pflichten aus dieser Verordnung sensibilisieren und Beschwerden in Bezug auf derartige Datenverarbeitungsvorgänge bearbeiten sollten.**

Was ist zu tun?

Für die Verarbeitung von personenbezogenen Daten bei der Ausübung justizieller Tätigkeiten durch die Gerichte sollte eine justizeigene unabhängige Kontrollstelle im Sinne des Erwägungsgrunds 20 der DSGVO eingerichtet werden.

4.4 Soziales

Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden (Sozialgeheimnis). Die Verarbeitung von Sozialdaten setzt eine ausreichende Befugnis voraus, die sich aus einer Rechtsvorschrift oder der Einwilligung des Betroffenen ergeben kann. Der Leistungsträger muss ausreichende technische und organisatorische Maßnahmen zum Schutz der Sozialdaten treffen. Die Anforderungen an den Schutz der Sozialdaten sind hoch.

4.4.1 Online-Prüfung von Sozialdaten – nur unter besonderen Bedingungen möglich

Wie können Rechnungshöfe Prüfungen durchführen, wenn es z. B. wegen Corona nicht möglich ist, die zu prüfende Stelle aufzusuchen? Können Prüfungen auch online durchgeführt werden?

Rechnungshöfe müssen bei Prüfungen unter Umständen auch auf Sozialdaten zugreifen. Bei einer Prüfung vor Ort ermöglicht die geprüfte Stelle dem Prüfer, Akten zu lesen, oder erteilt den Zugriff auf IT-Verfahren, die von der geprüften Stelle eingesetzt werden, um die Sozialdaten digital zu verarbeiten. Die geprüfte Stelle behält also die Kontrolle darüber, welche Sozialdaten wann den Prüfern zugänglich sind. Diese Kontrollbefugnis der geprüften Stelle muss auch bei einer Online-Prüfung sichergestellt werden.

Gemeinsam mit dem Landesrechnungshof wurden folgende Rahmenbedingungen definiert:

- Die geprüfte Stelle wird vorab detailliert über den beabsichtigten Umfang der Datenerhebung informiert.
- Der Zeitraum des Online-Zugriffs wird vorab festgelegt.
- Der Zeitpunkt und der Zeitrahmen eines jeweiligen Online-Zugriffs werden vorab der geprüften Stelle – aufgeschlüsselt nach Tagen/Uhrzeiten (von … bis) – mitgeteilt.
- Der Umfang der Datenerhebung bei einem Online-Zugriff wird auf den Umfang der Datenerhebung vergleichbar einer Prüfung vor Ort begrenzt.
- Bei Online-Zugriffen sind ausschließlich lesende Zugriffe zu Prüfzwecken möglich. Sofern Reports, Berichte, Auswertungen o. Ä. erzeugt werden, dürfen diese die zugrunde liegenden Datenbestände nicht verändern.
- Ein Datenexport oder die Duplizierung von Daten erfolgt ausschließlich in Kenntnis der geprüften Stelle.
- Soweit eine Online-Prüfung mittels Fernzugriff auf die Datenbestände der geprüften Stelle erfolgt, muss durch eine sichere Authentifizierung sichergestellt werden, dass nur die Prüfenden Zugriff erhalten. Dies erfordert
  1. eigene Nutzerkonten für die Prüfenden mit ausreichend komplexen Passwörtern oder anderen Nachweisen der Berechtigung,
  2. Zugriffe über das Landesnetz oder besondere Sicherungen (Verschlüsselung, Zwei-Faktor-Authentifizierung) bei Zugriffen über das Internet,
  3. keine dauerhafte Freischaltung der Zugriffsmöglichkeit, sondern Freischaltung durch die geprüfte Stelle nach Absprache.

  Alternativ wäre denkbar, eine elektronische Prüfung in den Räumlichkeiten der geprüften Stelle vorzunehmen (etwa an einem Prüfungsarbeitsplatz, der Zugriffe auf die elektronischen Datenbestände erlaubt, aber den Kontakt mit der geprüften Stelle minimiert).

  Eine weitere Möglichkeit besteht darin, dass die ausgewählten Daten kopiert und auf einen Datenträger exportiert in die Systeme der Prüfstelle importiert werden, mit denen dann die Prüfung erfolgt.
- Es erfolgt eine Protokollierung von Online-Zugriffen bei der geprüften Stelle.

  Sofern im Rahmen der Prüfung personenbezogener Daten eine Auswahl von Daten erfolgen soll (z. B. Stichproben), jedoch eine technische Beschränkung des Zugriffs auf diese Daten (z. B. Kopie der ausgewählten Daten, Einräumung entsprechend zugeschnittener Leserechte) nicht möglich wäre, wäre durch eine Online-Prüfung im Ergebnis ein vollständig wahlfreier und nicht überwachter

Zugriff auf sämtliche Datenbestände möglich (vergleichbar mit der Überlassung eines Generalschlüssels). Um in diesen Fällen eine vergleichbare Situation zu einer Vor-Ort-Prüfung zu schaffen, bietet eine Eingriffsmöglichkeit der geprüften Stelle in den Prüfungsvorgang (z. B. durch ein „Schattenterminal“ oder die „Spiegelung“ eines Online-Zugriffs, mit der Möglichkeit der Deaktivierung des Zugriffs) Abhilfe.

Was ist zu tun?

Bevor die Möglichkeit einer Online-Prüfung von Sozialdaten eröffnet wird, sind von der geprüften Stelle die zuvor aufgezeigten Rahmenbedingungen sicherzustellen.

4.4.2 Vorlagepflicht von Kontoauszügen – die letzten drei Monate reichen!

Wer Sozialleistungen wie Wohngeld, Grundsicherung oder Arbeitslosengeld beantragt, wird zumeist aufgefordert, die Kontoauszüge der letzten drei Monate im Amt vorzulegen. Hierfür bedarf es keiner besonderen Begründung der Behörde. Vereinzelt wurde uns jedoch – und das nicht nur aus Schleswig-Holstein – berichtet, dass Hilfesuchende ohne besonderen Grund aufgefordert wurden, die Kontoauszüge der letzten sechs Monate vorzulegen. Das geht zu weit.

In der Rechtsprechung (u. a. BSG 19.09.2008, B 14 AS 45/07 R) wird vertreten, dass die Kontoauszüge der letzten drei Monate vorzulegen sind. Datenschutzaufsichtsbehörden weisen seit Jahren darauf hin, dass besondere Gründe vorliegen müssen, damit die Vorlage von Kontoauszügen über einen Zeitraum von mehr als drei Monaten gefordert werden darf. Das ULD hat hierzu Hinweise für die datenschutzgerechte Gestaltung der Anforderung von Kontoauszügen veröffentlicht:

https://www.datenschutzzentrum.de/medizin-soziales/

Kurzlink: *https://uldsh.de/tb39-4-42*

An dieser Rechtsauffassung hat sich auch nichts geändert, nur weil die Behörden neuerdings Leistungen für bis zu zwölf Monate bewilligen können. Hilfesuchende sind zudem auf die (begrenzte) Möglichkeit der Schwärzung von Buchungstexten hinzuweisen. Die Anforderung ungeschwärzter Kontoauszüge muss begründet werden.

Was ist zu tun?

Sozialleistungsträger müssen bei der Aufforderung zur Vorlage von Kontoauszügen den Grundsatz der Erforderlichkeit der Datenerhebung beachten. In der Regel ist es ausreichend, wenn Hilfesuchende aufgefordert werden, die Kontoauszüge der letzten drei Monate im Amt vorzulegen.

4.5 Schutz des Patientengeheimnisses

4.5.1 Prüfung einer Gesundheitseinrichtung – Mängel müssen abgestellt werden

Die Datenschutzüberprüfung eines Klinikums bezog sich auf die Umsetzung der technischen und organisatorischen Maßnahmen zum Schutze der Patientendatenverarbeitung. Es wurden stichprobenartig u. a. folgende Bereiche geprüft:

- Organisationsstrukturen des Klinikums mit Zuständigkeiten und Verantwortlichkeiten,
- Funktion des Datenschutzmanagements,
- Einhaltung von anerkannten und empfohlenen Standards zum Schutz der Patientendaten,
- Zugriffs- und Berechtigungsmanagement,
- Sicherheitsfunktionen der eingesetzten IT-Systeme,
- Absicherung der verwendeten internen und externen Netze für die Datenkommunikation,
- Schutz der Patientendaten im Rahmen der Auftragsverarbeitung,
- Nachvollziehbarkeit und Protokollierung von Zugriffen auf Patientendaten,
- Datensicherung und Datenlöschung,
- Dokumentation und Nachweise zur Einhaltung und Überwachung der Datenschutzvorschriften.

Die Überprüfung hat ergeben, dass die Verantwortlichen des Klinikums der Einhaltung datenschutzrechtlicher Anforderungen der DSGVO und des BDSG keinen angemessenen Stellenwert zuordneten. Demzufolge wurde festgestellt, dass die Verarbeitung von Patientendaten erhebliche Schwachstellen aufwies. Nachfolgend ein kurzer Auszug aus unserem dem Klinikum zugestellten Prüfbericht:

- Ein Datenschutzmanagement, das die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch plant, umsetzt und kontrolliert, ist im Klinikum nicht ausreichend integriert. Die Verantwortlichen und der bestellte Datenschutzbeauftragte befolgten ihre gemäß der DSGVO auferlegten Pflichten nicht im gebotenen Maße.
- Die für Kliniken und Krankenhäuser von den Datenschutzbeauftragten des Bundes und der Länder erstellte „Orientierungshilfe Krankenhausinformationssysteme“ (OH KIS) wurde von den Verantwortlichen des Klinikums nicht beachtet.
- Sehr viele Beschäftigte des Klinikums verfügten über zu weitreichende Zugriffsrechte bezüglich der Patientendaten und konnten unkontrolliert auf den Datenbestand des Klinikums zugreifen.
- Die Archivräume für Patientenakten wurden zum Teil nicht ordnungsgemäß geführt. Unbefugte Kenntnisnahmen von Daten in Patientenakten durch Beschäftigte des Klinikums konnten nicht ausgeschlossen werden.
- Mehrere Dienstleister konnten ohne nachvollziehbare Weisung und Kontrolle der Verantwortlichen des Klinikums tätig werden und auf Patientendaten uneingeschränkt zugreifen. Verträge im Rahmen der Auftragsverarbeitung konnten nicht für alle Dienstleister vorgelegt werden.
- Die Server- und Technikräume vermittelten den Eindruck einer nicht ordnungsgemäßen Betriebsführung. Aufgrund unzureichender technischer und organisatorischer Maßnahmen konnte der Schutz personenbezogener Daten auf den im Klinikum eingesetzten Arbeitsstationen und zentralen IT-Komponenten nicht angemessen gewährleistet werden.
- Ferner wurde über Jahre hinweg versäumt, veraltete Betriebssysteme auf aktuelle Betriebssysteme zu migrieren. Auf den Arbeitsstationen und Servern wurden überwiegend veraltete und nicht mehr dem Stand der Technik entsprechende Betriebssysteme eingesetzt.
- Ein geregeltes Verfahren zur Protokollierung und der damit verbundenen Nachvollziehbarkeit der Patientendatenzugriffe durch Beschäftigte des Klinikums war für die im Klinikum eingesetzten IT-Komponenten nicht implementiert.
- Die mit MS-Office angelegten Dateiablagen mit Patientendaten waren nicht prüffähig. Die vorgefundenen Strukturen vermittelten den Eindruck einer unsystematischen Nutzung durch Beschäftigte des Klinikums. In mehreren verschachtelten Ablagen wurden Tausende von Dateien gefunden. Für die

Einrichtung der Ablagestrukturen sowie für die Vergabe von Berechtigungen gab es keine nachvollziehbaren Vorgaben.

- Für die meisten Fachanwendungen mit Patientendaten konnten die Verantwortlichen des Klinikums keine Berechtigungskonzepte für den Zugriff auf personenbezogene Daten vorlegen.
- Ferner wurde von ihnen versäumt, für Datenverarbeitungen, die hohe Risiken für Patientinnen und Patienten zur Folge haben könnten, eine Datenschutz-Folgenabschätzung durchzuführen.

„Orientierungshilfe Krankenhausinformationssysteme“:

https://www.datenschutzzentrum.de/artikel/1107-OH-KIS-Orientierungshilfe-Krankenhausinformationssysteme.html

Kurzlink: *https://uldsh.de/tb39-4-51*

Was ist zu tun?

Das Klinikum ist aufgefordert, die Datenschutzmängel schnellstmöglich abzustellen. Dafür ist es erforderlich, dass der Verantwortliche des Klinikums für die Steuerung der Datenschutz- und Informationssicherheitsprozesse ein Datenschutzmanagement implementiert. Es wird empfohlen, die für Krankenhäuser anerkannten Standards für Datenschutz und Informationssicherheit, insbesondere die „Orientierungshilfe Krankenhausinformationssysteme“, zu beachten.

4.5.2 Online-Terminvereinbarung – verschlüsselte Anfrage, unverschlüsselte Antwort?

Wer kennt das nicht, man will schnell noch einen Termin vereinbaren, aber das Telefon der Arztpraxis ist dauernd besetzt. Wie gut, dass die Praxis auch eine Online-Terminvereinbarung anbietet. Also Smartphone gezückt, ab ins Internet, Homepage der Arztpraxis aufgerufen, Online-Terminvereinbarung angeklickt, den eigenen Namen und vielleicht noch wo es wehtut eingegeben und auf „Senden“ gedrückt. Es dauert nicht lange, und schon erhält man den Termin. Alles ganz einfach. Aber auch sicher?

Verschiedene Firmen bieten Arztpraxen eine Software für eine Online-Terminvereinbarung an. Viele dieser Anwendungen bieten eine gesicherte Plattform, damit Patientinnen und Patienten ihren Terminwunsch der Arztpraxis mitteilen können, ohne dass Unbefugte hiervon Kenntnis nehmen können. Die Terminanfragen sind also geschützt. So weit, so gut. Aber wie sicher ist die Terminbestätigung?

Im letzten Jahr mussten wir wiederholt feststellen, dass die Terminbestätigung, also die Antwort der Arztpraxis an die Patientinnen und Patienten, häufig per unverschlüsselter E-Mail via Internet, also unsicher erfolgte (siehe auch Tz. 10.1). Die Terminbestätigung enthält regelhaft den Namen der anfragenden Person. Aber kein Unbefugter soll erfahren, wann wer zu welchem Arzt geht. Noch schlimmer ist es, wenn die Terminbestätigung Angaben zur Behandlung enthält. Möchten Sie, dass ein Psychiater Ihnen per Postkarte mitteilt, wann Sie das nächste Therapiegespräch wegen Ihrer Depression haben?

Die Verantwortung für die sichere Übermittlung der Terminbestätigung trägt die Ärztin oder der Arzt! Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, dass Unbefugte keine Kenntnis davon erhalten, wann wer warum in der Praxis einen Termin hat.

Wenn eine Arztpraxis einen externen Dienstleister mit der Online-Terminvereinbarung beauftragt, gilt es zudem zu bedenken, dass dies regelhaft eine sogenannte Auftragsverarbeitung darstellt. Diese

ist nur zulässig, wenn mit dem externen Dienstleister ein schriftlicher Auftragsverarbeitungsvertrag abgeschlossen wurde und die bei dem Dienstleister tätigen Personen auf das Datengeheimnis verpflichtet wurden.

Eine „Mustervereinbarung für einen Vertrag zur Auftragsverarbeitung“ haben wir in unserer Praxisreihe, Themenheft Nr. 3, veröffentlicht:

https://www.datenschutzzentrum.de/informationsmaterial/

Kurzlink: *https://uldsh.de/tb39-4-52*

Auch wenn einer sicheren Online-Terminvereinbarung aus datenschutzrechtlicher Sicht nichts entgegensteht, sollten Patientinnen und Patienten weiterhin alternative Möglichkeiten der Terminvereinbarung, z. B. per Telefon, angeboten werden.

Was ist zu tun?

Arztpraxen müssen beachten, dass sie auch bei der Online-Terminvereinbarung die Verantwortung für die sichere Übermittlung von Patientendaten tragen. Die Terminbestätigung darf nicht per unverschlüsselter E-Mail via Internet erfolgen. Wird ein Dienstleister mit der Online-Terminvereinbarung beauftragt, sind die gesetzlichen Anforderungen der Auftragsverarbeitung zu beachten.

4.5.3 Die erste Kopie der Patientenakte ist kostenfrei!

Es ist unstrittig, dass Patientinnen und Patienten nicht nur Auskunft über ihre Daten, sondern auch Einsicht in ihre Patientenakte verlangen dürfen. Nur in wenigen besonderen Fällen darf dies verweigert werden – z. B. wenn therapeutische Gründe entgegenstehen.

Patientinnen und Patienten können auch eine Kopie ihrer Patientenakte verlangen, egal ob die Daten in Papierform oder digital gespeichert sind. Im letzten Jahr schilderten uns die betroffenen Personen, dass in den Arztpraxen jedoch Geld für die Kopien verlangt wurde. Ist das zulässig? Eine heikle Frage, auf die wir eine eindeutige Antwort geben: Stützt der Patient sein Begehren auf Artikel 15 DSGVO, dann hat er einen Anspruch darauf, dass ihm die erste Kopie der Patientenunterlagen kostenfrei überlassen wird.

Zwar sehen die Berufsordnungen der Ärzte- und der Zahnärztekammer Schleswig-Holstein sowie § 630g Bürgerliches Gesetzbuch (BGB) vor, dass Ärztinnen und Ärzte für die Anfertigung von Kopien den Ersatz ihrer Kosten von den Patientinnen und Patienten verlangen können. Diese Regelungen haben jedoch keinen Vorrang vor den europarechtlichen Bestimmungen der DSGVO. Eine Einschätzung, die u. a. auch das Landgericht Dresden in einem Urteil vom 29.05.2020 vertritt (Az. 6 O 76/20). Diese Einschätzung wird im Übrigen auch von Datenschutzaufsichtsbehörden anderer Bundesländer geteilt.

Sollten Ärztinnen und Ärzte oder Zahnärztinnen und Zahnärzte weiterhin für die Anfertigung der ersten Kopie der Patientenunterlagen Geld von den Patientinnen und Patienten verlangen, so besteht die Möglichkeit, diese per Verwaltungsakt anzuweisen, dem Antrag der betroffenen Personen auf Ausübung der ihnen nach der DSGVO zustehenden Rechte zu entsprechen.

Was ist zu tun?

Patientinnen und Patienten ist die erste Kopie der Patientenunterlagen kostenfrei zu überlassen, wenn diese ihr Begehren auf Artikel 15 DSGVO stützen.

4.5.4 Kein Zugang für neugierige Patientinnen und Patienten

Auch im letzten Jahr ein Dauerbrenner: Neugierige Patientinnen und Patienten nutzen die Wartezeit und riskieren einen Blick auf den Computer der Arztpraxis. Kann eine neugierige Patientin oder ein neugieriger Patient Daten anderer Patienten sehen, dann droht der Arztpraxis Ärger.

Wer kennt diese Situation nicht? Man wird von der freundlichen Arzthelferin oder dem freundlichen Arzthelfer in das Behandlungszimmer geschickt. Frau bzw. Herr Doktor kommt ja gleich. Und schon ist man für einige Augenblicke allein. Neugierig schaut man sich um, und der Blick bleibt am Bildschirm vom Praxiscomputer hängen. Was werde ich wohl sehen, wenn ich die Computermaus bewege oder auf die Tastatur tippe?

Patientendaten, also Gesundheitsdaten, sind besonders sensibel und dürfen Unbefugten nicht zugänglich sein. Niemand lässt Bargeld offen in der eigenen Praxis herumliegen. Patientendaten sind oftmals noch viel wertvoller. Um Gegenstände zu stehlen, braucht man Hände, für heikle Informationen über andere Menschen reichen neugierige Augen (oder Ohren).

Die Ärztin oder der Arzt müssen als Verantwortliche in besonderem Maße dafür Sorge tragen, dass Patientendaten auch während des Praxisbetriebes vor neugierigen Ohren, Händen und Augen geschützt sind. Dies gilt auch bzw. gerade für den Zugang zu digitalen Patientendaten. Wird eine Patientin oder ein Patient in einem Raum mit einem Praxisrechner allein gelassen, so muss der Rechner gegen einen unbefugten Zugriff geschützt sein. Wird der Raum verlassen, ist der Rechner zu sperren. Ein passwortgeschützter Bildschirmschoner kann helfen. Moderne Praxen statten ihre Mitarbeiterinnen und Mitarbeiter mit einem Token aus, damit der Rechner automatisch gesperrt wird, wenn sie den Raum verlassen.

Selbstverständlich sind auch Papierunterlagen zu schützen und Arzt-Patienten-Gespräche diskret zu führen. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat gemeinsam mit der Ärztekammer und der Zahnärztekammer Schleswig-Holstein einen Datenschutz-Selbstcheck für Praxen erstellt, der unter dem folgenden Link abrufbar ist:

https://www.datenschutzzentrum.de/medizin-soziales/

Kurzlink: *https://uldsh.de/tb39-4-54*

Dieser Datenschutz-Selbstcheck hilft dabei, Patientendaten vor neugierigen Augen, Ohren und Händen zu schützen.

Was ist zu tun?

Patientendaten müssen besonders vor den neugierigen Augen, Ohren und Händen Unbefugter geschützt werden. Patientinnen und Patienten dürfen daher nicht mit Praxisrechnern alleine gelassen werden, wenn diese nicht anderweitig gegen einen unbefugten Zugriff geschützt sind.

4.5.5 Postversand von Patientendaten auf CD – bitte verschlüsselt!

Aus vielen Gründen müssen Patientendaten verschickt, also übermittelt werden. Umständlich werden Arztbriefe oder ganze Akten ausgedruckt und in Papierform mit der Post versandt. Will der Empfänger die Daten elektronisch weiterverarbeiten, müssen die Unterlagen wieder aufwendig eingescannt werden. Digitale Datenkopien auf einem mobilen Datenträger wie einer CD oder einem USB-Stick mit der Post zu verschicken wäre einfacher. Aber ist das auch zulässig?

Ja! Das Auskunftsrecht der betroffenen Person und das Recht auf Datenübertragbarkeit sehen diese Möglichkeit sogar ausdrücklich vor.

Allerdings gilt es zu beachten, dass der Verantwortliche bei Patientendaten aufgrund ihrer Sensibilität im besonderen Maße dafür Sorge zu tragen hat, dass diese nicht nur rechtmäßig, sondern auch vertraulich übermittelt werden. Durch geeignete technische und organisatorische Maßnahmen ist ein ausreichender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sicherzustellen.

Es ist kein Geheimnis, dass die Post nicht immer beim gewünschten Empfänger ankommt. Manchmal reißen auch Versandumschläge auf, sodass dann Datenträger herausfallen können. Anders als Papierunterlagen können digitale Daten auf einer CD oder einem USB-Stick verschlüsselt werden. Bei Verlust der Postsendung sind die Daten dann für Unbefugte nicht lesbar. Der Versand bzw. die Übermittlung von digitalen Daten verringert also nicht nur den Arbeitsaufwand, sondern erhöht eindeutig die Datensicherheit, wenn die Daten auf dem mobilen Datenträger angemessen verschlüsselt werden. So kann man Datenpannen vermeiden, bei denen personenbezogene Daten im Klartext in falsche Hände geraten (siehe Tz. 4.5.9).

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein stellt entsprechende Informationen zur Verfügung:

https://www.datenschutzzentrum.de/technik/

Kurzlink: *https://uldsh.de/tb39-4-55*

Was ist zu tun?

Werden Patientendaten in digitaler Form mit einem mobilen Datenträger, z. B. per CD oder USB-Stick, mit der Post versandt, sollten die Daten angemessen verschlüsselt werden.

4.5.6 Anhörung für ein Landeskrankenhausgesetz

Im vergangenen Berichtszeitraum leitete das federführende Ministerium für Soziales, Gesundheit, Jugend, Familie und Senioren Schleswig-Holstein dem ULD den ersten Entwurf für ein Landeskrankenhausgesetz zu. In der daraufhin vorgenommenen Stellungnahme erläuterte das ULD wesentliche Punkte zur Anwendung datenschutzrechtlicher Vorschriften bei Krankenhäusern in öffentlicher und privater Trägerschaft, zur Auslagerung der Verarbeitung von Patientendaten auf externe Dienstleister, zur Datenverarbeitung für Forschungszwecke und zum Umfang der Auskunftsrechte von Patientinnen und Patienten (39. TB, Tz. 4.5.1). Einige wesentliche Punkte, für welche ein Änderungsbedarf aus datenschutzrechtlicher Sicht mitgeteilt wurde, fanden bei der Finalisierung des Gesetzentwurfs allerdings keine Berücksichtigung. Der entsprechende Entwurf (Drucksache 19/2042) ist abrufbar unter:

https://www.landtag.ltsh.de/infothek/wahl19/drucks/02000/drucksache-19-02042.pdf

Kurzlink: *https://uldsh.de/tb39-4-56a*

In der schriftlichen Anhörung zum Gesetzentwurf für das Landeskrankenhausgesetz erneuerte das ULD seine Hinweise zur notwendigen Anpassung einzelner Vorschriften im Abschnitt zum Patientendatenschutz und konkretisierte die darauf beruhenden Ausführungen (§§ 35-40 des Gesetzentwurfs). Die Stellungnahme ist abrufbar unter:

https://www.landtag.ltsh.de/infothek/wahl19/umdrucke/04100/umdruck-19-04175.pdf

Kurzlink: *https://uldsh.de/tb39-4-56b*

Maßgeblich waren insbesondere folgende Punkte:

- **Daten von „Angehörigen oder anderen Bezugspersonen der Patientinnen und Patienten sowie sonstiger Dritter" zählen nicht zu den Patientendaten.** Es bleibt offen, wer zu den „sonstigen Dritten" gehört. Patientendaten beziehen sich vielmehr auf Anamnesen, Diagnosen, Untersuchungen, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Besucherlisten, insbesondere Angaben zu Angehörigen, zählen nicht zu dieser Dokumentation. Ferner ist auch nicht zu rechtfertigen, patientenfremde Angaben der **langen Aufbewahrungsfrist** für Patientendaten zu unterwerfen.
- Vorgesehen ist eine **Verarbeitung von Patientendaten „zur Überprüfung der Tätigkeit der Mitarbeiterinnen und Mitarbeiter des Krankenhauses"**. Das ULD empfahl nachdrücklich die Streichung dieser Norm, zumal für Krankenhäuser in privatrechtlicher Organisationsform vorrangig Bundesrecht zu beachten ist (§ 26 BDSG). Weder für den Medizinischen Dienst der Krankenversicherung (MDK) noch für die Krankenhäuser in ihrer Funktion als Arbeitgeber ist eine Bestimmung erforderlich, um eine Datenverarbeitung „zur Überprüfung von Mitarbeiterinnen und Mitarbeitern" zu regeln. Für Prüfungen des MDK und Mitwirkungspflichten der Arbeitgeber bestehen vorrangige bundesrechtliche Bestimmungen (§§ 275a, 276 SGB V).
- Der Gesetzentwurf legitimiert ohne weitere Voraussetzungen eine Verarbeitung pseudonymisierter Daten, soweit eine Verarbeitung von Patientendaten nicht erforderlich sein sollte. Nicht berücksichtigt wird dabei, dass es sich nach den vorrangigen europäischen Vorgaben der DSGVO bei **pseudonymisierten Daten** auch um personenbezogene Daten handelt, **deren Verarbeitung einer Rechtsgrundlage bedarf**. Daher bat das ULD auch hier um Streichung der entsprechenden Formulierung.
- Nach Abschluss der Behandlung sollen personenbezogene Daten der Patientinnen und Patienten dem **alleinigen Zugriff der „jeweiligen Fachabteilung"** unterliegen. Der Gesetzentwurf gibt keinen Aufschluss darüber, welcher konkrete Bereich und Personenkreis mit einer „Fachabteilung" gemeint ist. Unberücksichtigt bleiben dabei auch die unter den deutschen Datenschutzaufsichtsbehörden abgestimmten und bewährten Grundsätze in der **„Orientierungshilfe Krankenhausinformationssysteme" (OH KIS)**.

„Orientierungshilfe Krankenhausinformationssysteme":

https://www.datenschutzzentrum.de/uploads/medizin/OH_KIS.pdf

Kurzlink: *https://uldsh.de/tb39-4-56c*

Leider hat der Gesetzgeber die obigen Hinweise bei der Schaffung des Landeskrankenhausgesetzes nicht berücksichtigt (GVOBl. Schl.-H., Nr. 22 vom 23.12.2020, Seite 1.004 ff.). Dabei gab das ULD bereits in seiner damaligen Stellungnahme zu bedenken, dass der vorliegende Gesetzentwurf im Falle der Beschließung und Beibehaltung der zur Streichung empfohlenen Passagen zu gewichtigen Problemen in der Anwendungspraxis führen kann.

Was ist zu tun?

Der aufgezeigte Änderungsbedarf sollte bei einer späteren Novellierung des Landeskrankenhausgesetzes bedacht werden.

4.5.7 Änderung des Maßregelvollzugsgesetzes: Nachbesserung durch den Landtag

Im letzten Tätigkeitsbericht hatten wir über den Gesetzentwurf zur Änderung des Maßregelvollzugsgesetzes berichtet (38. TB, Tz. 4.5.7). Mittlerweile hat der Landtag das Gesetz beschlossen. Nach Durchführung einer Sachverständigenanhörung im Sozialausschuss, an der wir uns beteiligt haben, hat der Landtag zahlreiche Änderungen an der Gesetzesvorlage vorgenommen. Damit hat er den von uns aufgezeigten Änderungsbedarf in weiten Teilen umgesetzt.

Unter anderem sind die Vorschriften über den Einsatz von Videotechnik zur Beobachtung bestimmter Bereiche in der Maßregelvollzugseinrichtung deutlich verbessert worden. Hier hat der Landtag unsere Empfehlung aufgegriffen und die Regelung an die des Justizvollzugsdatenschutzgesetzes angeglichen.

Nicht geändert wurde dagegen die Regelung zum Auskunftsanspruch in § 43 des Maßregelvollzugsgesetzes (MVollzG). Wie bereits im 38. Tätigkeitsbericht erläutert, greift die Vorschrift für eine Umsetzung des europarechtlichen Auskunftsanspruchs der betroffenen Personen zu kurz. Die Vorschrift ist allerdings so weit gefasst, dass sie als allgemeine Regelung zur Akteneinsicht verstanden werden kann, die keine gegenüber dem Landesdatenschutzgesetz vorrangige Regelung zum Auskunftsanspruch betroffener Personen nach dem Datenschutzrecht trifft. Geregelt werden in § 43 MVollzG Auskunfts- und Akteneinsichtsrechte nicht nur der betroffenen Personen. Festgelegt werden Akteneinsichtsrechte der Verteidiger von Untergebrachten und des Europäischen Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (CPT), des Unterausschusses der Vereinten Nationen zur Prävention von Folter (SPT) sowie der Nationalen Stelle zur Verhütung von Folter. Bei diesen Rechten handelt es sich nicht um Datenschutzrechte. Es geht vielmehr um die Verfahrensrechte der Untergebrachten und um Kontrollrechte der Antifolterstellen. Ein Bezug zum Datenschutzrecht ergibt sich nur aus dem Standort der Vorschrift im dritten Teil des Gesetzes, der dem Datenschutz gewidmet ist. Da in der Vorschrift aber Sachverhalte geregelt werden, die nicht dem Datenschutzrecht zuzuordnen sind, ist dem Standort keine besondere Bedeutung zuzumessen.

Im Ergebnis lässt sich die Vorschrift europarechtskonform dahin gehend auslegen, dass sie verfahrensrechtliche Ansprüche der betroffenen Personen regelt, jedoch keine oder zumindest keine abschließende Regelung über deren datenschutzrechtlichen Auskunftsanspruch trifft. Dieser ergibt sich vielmehr aus dem allgemeinen Datenschutzrecht. Eine solche Auslegung ist mit der Systematik des Maßregelvollzugsgesetzes vereinbar und stellt eine europarechtskonforme Anwendung des Landesrechts sicher. Das bedeutet: Das Auskunftsrecht des Datenschutzrechts können (selbstverständlich) auch untergebrachte Personen in Anspruch nehmen.

4.5.8 Datenpannen im Medizinbereich

Bei einer Datenpanne hat der Verantwortliche die Pflicht, diese Datenschutzverletzung möglichst innerhalb von 72 Stunden der Aufsichtsbehörde zu melden. Neben Angaben dazu, wie es zu der Datenpanne kommen konnte, muss geschildert werden, in welchem Umfang welche Daten und wie viele Personen betroffen sind. Zudem müssen die wahrscheinlichen Folgen der Datenschutzverletzung ebenso wie die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und zur Abmilderung der möglichen nachteiligen Auswirkungen für die betroffenen Personen beschrieben werden. Nicht fehlen dürfen Angaben zum Datenschutzbeauftragten. Im letzten Berichtsjahr erreichten uns aus unterschiedlichsten medizinischen Praxen und Krankenhäusern eine Vielzahl von Meldungen. Jetzt gilt es, aus diesen Fehlern zu lernen und Sorge zu tragen, dass dies nicht erneut passieren kann.

4.5.9 Gemeldete Datenpannen: Fehlversand von Patientenunterlagen

Der Fehlversand von Patientenunterlagen stellt eine der häufigsten Ursachen für eine Datenschutzverletzung dar. Hier einige Beispiele:

- Bei dem Versand per Fax vertippt sich die Mitarbeiterin oder der Mitarbeiter, wählt die falsche Kurzwahlnummer oder verwendet eine veraltete Faxnummer.
- Beim Postversand wird eine falsche Anschrift verwendet. Schon die Angabe einer falschen Hausnummer kann dazu führen, dass der Brief im falschen Briefkasten landet.
- Wenn zu viele Postausgänge auf einmal bearbeitet werden, kommt es zu Überkreuzverwechslungen oder Unterlagen von zwei verschiedenen Patientinnen oder Patienten landen in einem Briefumschlag.
- Werden Unterlagen persönlich ausgehändigt, kann es zu Verwechslungen kommen. Patientinnen oder Patienten erhalten Unterlagen anderer behandelter Personen.
- Newsletter oder Informationsschreiben werden per offenem E-Mail-Verteiler versandt. So erhalten die Adressatinnen und Adressaten Kenntnis von der Identität anderer Empfängerinnen oder Empfänger/Patientinnen oder Patienten.
- Bei elektronischen Patientenakten kann die Vergabe eines falschen Zugangscodes dazu führen, dass Unbefugte Zugang zu fremden Patientendaten erhalten.

Was ist zu tun?

Patientendaten sind besonders sensibel. Verantwortliche müssen daher auch bei dem Versand von Patientenunterlagen sorgfältig darauf achten, dass diese nicht aus Versehen in falsche Hände geraten.

4.5.10 Gemeldete Datenpannen: Diebstahl, Einbruch, Hackerangriff in der Arztpraxis

Nicht immer liegt die Ursache für eine Datenpanne in einem vorsätzlichen Fehlverhalten des Verantwortlichen. So manches Unheil droht auch von außen. Es ist erschreckend, in wie vielen Fällen uns im letzten Jahr von Einbrüchen, Diebstählen oder Hackerangriffen berichtet wurde, von denen auch Patientendaten betroffen waren. Hier einige Beispiele:

- Einbruch in der Arztpraxis: Gestohlen wurde u. a. ein Laptop mit Patientendaten. Leider waren die Daten auf dem Laptop nicht verschlüsselt.
- Einbruch und Vandalismus in einer anderen Arztpraxis: Gestohlen wurde nichts. Aber die Praxisräume wurden verwüstet. Unter anderem wurden die Aktenschränke aufgebrochen und die darin befindlichen Patientenakten herausgerissen. Zwar fehlte keine Akte, aber ob die Täter einige Akten gelesen oder gar fotografiert haben, ließ sich nicht feststellen.
- Während des normalen Praxisbetriebs wurden EKG-Geräte gestohlen. Besonders ärgerlich, weil auf den gestohlenen Geräten noch die Daten und Messwerte von Patientinnen und Patienten gespeichert waren.
- Ambulante Pflegedienste müssen Patientenunterlagen mit dem Auto transportieren. Doppelt ärgerlich ist es, wenn so ein Fahrzeug aufgebrochen oder gestohlen wird und der Dieb darin Patientenunterlagen findet.
- Ein weiterer Dauerbrenner waren auch im letzten Jahr Angriffe auf die IT von Arztpraxen mit sogenannten Verschlüsselungstrojanern (38. TB, Tz. 6.3.4). Verschlüsselungstrojaner haben zwar (zunächst) nicht das Ziel, Patientendaten auszuspionieren, auszuschließen ist dies jedoch nicht.

Was ist zu tun?

Ein ausreichender Einbruchschutz muss für Arztpraxen genauso selbstverständlich sein wie die erforderlichen Maßnahmen zur IT-Sicherheit.

4.5.11 Dumm gelaufen – noch mehr Datenpannen

Es gibt Datenpannen, da muss auch der erfahrenste Datenschützer schmunzeln. Andererseits gibt es auch Datenpannen, die einen fassungslos machen. Beispiele gefällig?

- Endlich Feierabend in der Arztpraxis. Eine Mitarbeiterin wird gebeten, auf dem Heimweg noch schnell die Briefe zur Post zu bringen. Wer kennt es nicht? Man steht vor seinem Auto, hat die Hände voll und der Autoschlüssel ist ganz unten in der Tasche. Schnell die Briefe aufs Autodach gelegt, aufgeschlossen, eingestiegen und losgefahren. Da war doch noch was? Richtig … die Post auf dem Autodach. Zu spät. Nicht alle Briefe wurden trotz intensiver Suche gefunden. Dumm gelaufen.

- Die Ex-Frau wird im Krankenhaus behandelt und der Ex-Mann arbeitet in dem gleichen Krankenhaus als Physiotherapeut. So kann er – obwohl er nicht in die Behandlung seiner Ex-Frau eingebunden ist – die Patientenakte seiner Ex-Frau lesen. Die Dinge, die er auf diese Weise erfährt, nutzt er für den Streit um das Sorgerecht für das gemeinsame Kind. Erst als das bekannt wird, reagiert das Krankenhaus und überprüft die Leserechte von Physiotherapeuten (38. TB, Tz. 4.5.13). Und weil ihm das Krankenhaus fristlos kündigte, wurde aus dem Ex-Mann nun auch ein Ex-Mitarbeiter.

05

KERNPUNKTE

Straßenaufnahmen im Auftrag der Stadtwerke

Prüfung von Partnervermittlungen

Coronamaßnahmen – datenschutzkonform?

Datenpannen in der Wirtschaft

Videoüberwachung

5 Datenschutz in der Wirtschaft

Datenschutz im nichtöffentlichen Bereich macht einen Großteil der Beschwerden und Prüffälle aus. In diesem Kapitel zeigen wir die Bandbreite der Verfahren, mit denen wir uns beschäftigen. Dazu gehören grundsätzliche Verfahren wie die Kamerafahrten durch die Straßen im Auftrag der Stadtwerke (Tz. 5.1), Prüfungen von Partnervermittlungen (Tz. 5.2), unsere Hinweise zur Pflicht, als Coronamaßnahme Kontaktdaten zeitweise vorzuhalten (Tz. 5.3), zahlreiche Einzelfälle (Tz. 5.4), gemeldete Datenpannen (Tz. 5.5) und Videoüberwachung (Tz. 5.6).

5.1 Panoramaaufnahmen durch Befahrungen im Auftrag der Stadtwerke

Das ULD wurde darauf aufmerksam, dass **mehrere Stadtwerke Vermessungsfahrten in den jeweiligen Stadt- und Gemeindegebieten** geplant hatten. Ziel dieser Vermessungsfahrten war es, mittels auf dem Dach eines Autos angebrachter **3-D-Kameras und -Laserscanner** Panoramaaufnahmen zu erstellen, die zur **Generierung dreidimensionaler Straßenkarten** verwendet werden sollten. Diese Straßenkarten sollten durch die Mitarbeiterinnen und Mitarbeiter der Stadtwerke u. a. zur Messung und Planung von Bauprojekten sowie bei anstehenden Arbeiten an den Hausanschlüssen genutzt werden. Neben den Straßen und Gehwegen sollten auch die Häuserfronten und Vorgärten aufgenommen werden. Die Vermessungsfahrten sollten durch einen Dienstleister, der sich auf diese Art von Vermessungsfahrten spezialisiert hat, durchgeführt werden. Teilweise waren die Vermessungsfahrten auch schon abgeschlossen.

Bei der Aufnahme und der Verwendung der Bilder der Häuserfronten sowie der Vorgärten handelt es sich um eine Verarbeitung personenbezogener Daten, bei der die datenschutzrechtlichen Bestimmungen einzuhalten sind.

Aufgrund der erlangten Erkenntnisse haben wir ein aufsichtsbehördliches Verfahren eröffnet, in dem die Stadtwerke zur Stellungnahme aufgefordert wurden. Hierbei ging es insbesondere um die Klärung der Fragen, **auf welcher Rechtsgrundlage** die Verarbeitung erfolgte und wie die zahlreichen Betroffenen über die Vermessungsfahrten **informiert** wurden.

Im Laufe des aufsichtsbehördlichen Verfahrens stellte sich heraus, dass die betroffenen Personen teilweise nur unzureichend über die Erhebung ihrer personenbezogenen Daten informiert wurden bzw. nur unzureichende Maßnahmen geplant waren.

Informationspflichten

Bei der Erhebung personenbezogener Daten bei der betroffenen Person sind die Informationspflichten aus Artikel 13 DSGVO zu erfüllen. Der Betroffene muss hier u. a. über sein Widerspruchsrecht gegen die Verarbeitung informiert werden.

Es erfolgten lediglich unzureichende Hinweise auf den Webauftritten der Stadtwerke und des Dienstleisters sowie vereinzelte Anzeigen in der lokalen Presse. Es fehlten z. B. teilweise

- Informationen zu den Zwecken der Verarbeitung, d. h., aus welchen Gründen die Grundstücke fotografiert werden,
- Informationen über die Rechtsgrundlagen für die Anfertigung der Aufnahmen, um den Bürgerinnen und Bürgern eine nachvollziehbare Prüfung zu ermöglichen, ob eine Befugnis der Stadtwerke besteht,
- Informationen über die Speicherfristen,
- Informationen zu den Rechten betroffener Bürgerinnen und Bürger, einer Verarbeitung von Grundstücksaufnahmen widersprechen zu können,
- verständliche Angaben zu Widerspruchsrechten, denn durch falsche Verlinkungen entstand der Eindruck, dass eine Veröffentlichung der Grundstücksaufnahmen geplant sei,
- klare Verantwortlichkeiten, denn es wurde nicht deutlich, welche Rolle die Stadtwerke und welche Verantwortung der beauftragte Dienstleister übernimmt.

Wir bemängelten zudem, dass auf den genannten digitalen Kanälen insbesondere der ältere Teil der betroffenen Personen nicht verlässlich erreicht werden würde, da nicht generell seitens des Verantwortlichen unterstellt werden könne, dass diese Personen regelmäßig das Internet nutzen und dabei auch noch den Webauftritt der Stadtwerke aufrufen. Insgesamt erschien es nicht plausibel, dass selbst Kundinnen und Kunden, die das Internet nutzen, regelmäßig die Webauftritte der Stadtwerke besuchen und dabei etwaige Hinweise zu Befahrungen und der Anfertigung von Aufnahmen zur Kenntnis nehmen würden. Es kam erschwerend hinzu, dass die Befahrungen in einigen Fällen nur mit einem kurzen zeitlichen Vorlauf angekündigt wurden.

Dies führte zu unserer Anordnung gegenüber den Stadtwerken, den Informationspflichten der DSGVO nachzukommen, da die bisher getroffenen Maßnahmen nicht ausreichend waren, um die Betroffenen zu informieren. Die Ausgestaltung der Information sollte in der Form erfolgen, dass auch diejenigen informiert würden, die keinen digitalen Zugang haben oder das Internet nur unregelmäßig nutzen. Die Erfüllung der angeordneten Maßnahmen sowie eine hinreichende Erläuterung zur Rechtsgrundlage für die Verarbeitung der Aufnahmen waren Voraussetzung für die geplante Verarbeitung der Panoramaaufnahmen durch die Stadtwerke.

Die Stadtwerke setzten die angeordneten Maßnahmen fristgerecht um. Als Maßnahmen zur Bekanntgabe der **Pflichtinformation** gegenüber den Bürgerinnen und Bürgern wurden mehrere **Anzeigen in der lokalen Presse sowie Brief- und Postwurfsendungen** gewählt, sodass diesen in geeigneter Art und Weise die Informationen gemäß Artikel 13 DSGVO zur Verfügung gestellt wurden.

5.2 Prüfung von Partnervermittlungen: Einsatz von Listbrokern für Werbung

Aufgrund zahlreicher Beschwerden wurden im Berichtszeitraum acht Unternehmen geprüft, die ihre Webseiten im Bereich der **Partnervermittlung unter Verwendung von E-Mail-Newslettern** bewerben. Die geprüften Unternehmen beauftragen **für die Gewinnung von Neukunden häufig im Ausland ansässige Listbroker**, die die gewünschte **Werbung** unter Nutzung eigener Adressbestände versenden. Für den Empfänger ist es dabei **kaum nachvollziehbar**, aus welchem Grund er die Werbung erhält und an wen er sich zur Geltendmachung seiner Betroffenenrechte wenden kann.

Auch wenn der Erwägungsgrund 47 zur Datenschutz-Grundverordnung die Verarbeitung personenbezogener Daten zum Zweck der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung anerkennt, so sind in der nach Art. 6 Abs. 1 Buchst. f DSGVO erforderlichen Interessenabwägung insbesondere auch die „vernünftigen Erwartungen der betroffenen Person“, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in den Abwägungsprozess einzubeziehen. Da die potenziellen Neukundinnen und Neukunden bisher noch keine Beziehung zu den Unternehmen hatten, konnten die Verantwortlichen nicht davon ausgehen, dass die E-Mail-Empfängerinnen und -Empfänger eine entsprechende Werbung für die jeweiligen Partnervermittlungen erwarten. Des Weiteren überwiegen die schutzwürdigen Interessen der betroffenen Person in der Regel immer dann, wenn nach den Vorschriften des Gesetzes gegen den unlauteren Wettbewerb (UWG) eine **unzumutbare Belästigung** anzunehmen ist.

Wettbewerbsrecht

Nach § 7 Abs. 2 Nr. 3 des Gesetzes über den unlauteren Wettbewerb (UWG) ist bei Werbung unter Verwendung elektronischer Post eine unzumutbare Belästigung stets anzunehmen, wenn keine vorherige ausdrückliche Einwilligung des Adressaten vorliegt. Für Werbung an Bestandskunden gelten nach § 7 Abs. 3 UWG entsprechende Ausnahmen.

Bei der Beurteilung der Verantwortlichkeit für eine solche Werbemaßnahme ist außerdem zu berücksichtigen, dass die geprüften Unternehmen zwar selbst keinen Zugriff auf die für den Versand der Werbung genutzten personenbezogenen Daten haben, die **Verwendung der Daten für die entsprechende Werbeaktion allerdings veranlassen und von dieser profitieren**.

Da die Unternehmen den Zweck der Werbemaßnahme festlegen und die Zielgruppe definieren, die beauftragten Listbroker jedoch über die Mittel zur

Durchführung der Werbemaßnahme in Form des Adressdatenbestands und der Möglichkeit der Selektion verfügen, werden die Zwecke und Mittel der Verarbeitung von beiden gemeinsam festgelegt. Demnach liegt eine **gemeinsame Verantwortlichkeit** nach Artikel 26 DSGVO vor. Wir mussten die geprüften Unternehmen in den aufsichtsbehördlichen Verfahren mehrfach darauf hinweisen, dass eine solche gemeinsame Verantwortlichkeit auch vorliegen kann, wenn sie selbst keinen Zugang zu den betreffenden personenbezogenen Daten haben.

Im Falle einer gemeinsamen Verantwortlichkeit ist nach Art. 26 Abs. 1 DSGVO eine Vereinbarung abzuschließen, aus der die jeweiligen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen hervorgehen muss. Des Weiteren ist in dieser Vereinbarung transparent festzulegen, wer welche Verpflichtung gemäß der Datenschutz-Grundverordnung erfüllt. Eine solche Vereinbarung konnte von keinem der Unternehmen vorgelegt werden.

Ungeachtet einer solchen Vereinbarung kann eine betroffene Person ihre Rechte allerdings gemäß Art. 26 Abs. 3 DSGVO immer gegenüber jedem Einzelnen der Verantwortlichen geltend machen. Im Rahmen der gemeinsamen Verantwortlichkeit sind die werbetreibenden Unternehmen darüber hinaus auch dafür verantwortlich, dass die für einen rechtmäßigen Versand von Werbe-E-Mails erforderlichen Einwilligungen tatsächlich vorliegen.

Bei der Auswahl eines Listbrokers kann von den werbetreibenden Unternehmen im Rahmen der **bestehenden Sorgfaltspflichten** zumindest erwartet werden, dass diese sich bei der Auswahl ihres Vertragspartners über die **vertragliche Zusicherung des Bestands solcher Einwilligungen** hinaus auch die **Verfahrensweise zur Erhebung der erforderlichen Einwilligung erläutern** lassen.

Im Rahmen der durchgeführten Verfahren wurde von verschiedenen Unternehmen die bisherige Zusammenarbeit mit Listbrokern beendet, da diese die im Rahmen der Prüfungen angeforderten Einwilligungen nicht nachweisen konnten. Ansonsten waren zahlreiche Hinweise auf **mutmaßliche Verstöße** und in Einzelfällen auch die Festsetzung von Zwangsmaßnahmen zur Durchsetzung von Auskunftsanordnungen und Betroffenenrechten erforderlich.

5.3 Coronamaßnahme Kontaktdatensammlung – wie geht's datenschutzkonform?

Parallel zum Tätigwerden der Landesregierung, die im Verordnungswege u. a. die Verpflichtung für bestimmte Einrichtungen geregelt hat, Kontaktdaten der Besucherinnen und Besucher zu erheben, haben wir gegenüber dem zuständigen Ministerium und der Öffentlichkeit deutlich gemacht, dass jede Coronamaßnahme datenschutzkonform sein muss und daher auch Datenschutzanforderungen in Bezug auf eine etwaige Sammlung von Kontaktdaten zu berücksichtigen sind. Zur Kontaktdatenerhebung verpflichtete Einrichtungen wurden entweder im Vorfeld beraten, wie sie den Vorgaben der Landesverordnung in datenschutzkonformer Art und Weise nachkommen können, oder – wenn notwendig – darauf hingewiesen oder angewiesen, die Erhebung von Kontaktdaten mit den datenschutzrechtlichen Vorgaben in Einklang zu bringen oder zu unterlassen.

Um von Anfang an Fehler im Umgang mit Kontaktdaten nach Möglichkeit zu vermeiden (siehe auch Tz. 5.4.1), haben wir Informationen für die Öffentlichkeit, betroffene Personen und Verantwortliche bereitgestellt (wie z. B. ein Musterformular zur Kontaktdatenerhebung) und diese Informationen an die sich stetig wandelnde Rechtslage angepasst. Die Informationen sind unter dem folgenden Link abrufbar:

https://www.datenschutzzentrum.de/corona/

Kurzlink: *https://uldsh.de/tb39-5-3a*

Wer nach der Verordnung zur Erhebung von Kontaktdaten verpflichtet ist, muss auch die Vorgaben der Datenschutz-Grundverordnung (DSGVO) erfüllen. Hierzu zählen insbesondere die Einhaltung von Informationspflichten nach Artikel 13 DSGVO, die Einhaltung von Löschregeln nach Artikel 17 DSGVO und die Erfüllung technischer und organisatorischer Anforderungen nach Artikel 32 DSGVO. Um den Informationsverpflichtungen nach Artikel 13 DSGVO nachzukommen, können sich die Verantwortlichen an unserer Veröffentlichung zu Informationspflichten in unserer Praxisreihe orientieren:

https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-4-Informationspflichten.pdf

Kurzlink: *https://uldsh.de/tb39-5-3b*

Ausgehend vom Erhebungsdatum sind die Daten nach der vorgesehenen Speicherdauer von aktuell vier Wochen endgültig zu löschen. Eine Pflicht zur Löschung ergibt sich nach Ablauf der Frist schon aus Artikel 17 der DSGVO.

Zu den Vorgaben, die sich aus der DSGVO ergeben, gehört es u. a., dass sicherzustellen ist, dass unbefugte Dritte keine Kenntnis von den erhobenen Daten erlangen. Hierzu müssen nach Artikel 24 und Artikel 32 DSGVO geeignete technische und organisatorische Maßnahmen ergriffen werden. **Von einer Erhebung mittels offen ausgelegter Listen ist daher abzusehen.**

Die erhobenen Daten dürfen nur auf Verlangen der zuständigen Behörde an diese übermittelt werden. Eine Verwendung **zu anderen Zwecken ist unzulässig** und wäre mangels Rechtsgrundlage ein bußgeldbewehrter Verstoß gegen die DSGVO.

Besteht eine gesetzliche Verpflichtung zur Erhebung von Kontaktdaten nach Landesrecht, darf der Besuch oder die Nutzung einer Einrichtung oder die Teilnahme an einer Veranstaltung untersagt werden, wenn erkennbar ist, dass die betroffenen Personen eine Erhebung der Kontaktdaten verweigern.

Betroffene Personen **dürfen** gemäß § 20 Personalausweisgesetz (PAuswG) ihren **Personalausweis** einsetzen, wenn sie dies möchten, um die Erhebung zu vereinfachen. Hierzu sind sie jedoch **nicht verpflichtet**.

§ 20 Abs. 1 PAuswG

Der Inhaber kann den Ausweis bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden.

Eine Erhebung und Speicherung personenbezogener Daten auf Vorrat ohne gesetzliche Verpflichtung auf Grundlage von Art. 6 Abs. 1 Buchst. f DSGVO zu Zwecken der Pandemiebekämpfung (Nachverfolgung von Infektionsketten) ist für die Einrichtungen nicht zulässig. Es überwiegen die Grundrechte und Freiheiten der betroffenen Personen, die eine Erhebung der sie betreffenden personenbezogenen Daten nicht dulden müssen, wenn eine dahin gehende Entscheidung des Gesetzgebers und der zuständigen Behörden nicht existiert. Es ist nämlich **Aufgabe des Gesetzgebers** festzulegen, welche Eingriffe in das Recht auf Schutz der Verarbeitung personenbezogener Daten als Coronamaßnahme geeignet, erforderlich und angemessen ist. Haben sich der Gesetzgeber und die zuständigen Behörden gegen eine solche Maßnahme zur Pandemiebekämpfung entschieden, ist es nicht privaten Stellen überlassen, die Entscheidung über eine solche Datenerhebung und deren Art und Weise zu treffen.

Denkbar wäre es allenfalls, eine Erhebung personenbezogener Daten auf Grundlage einer freiwilligen Einwilligung nach Artikel 7 DSGVO anzubieten. Würde der Besuch oder die Nutzung einer Einrichtung oder die Teilnahme an einer Veranstaltung verweigert für den Fall, dass nicht eingewilligt werden würde, ließe dies eine Einwilligung mangels **Freiwilligkeit** unwirksam werden.

Trotz der Hilfestellung über unsere Webseiten wurden uns immer wieder Datenschutzverstöße gemeldet, denen wir nachgegangen sind. Einige Bürgerinnen und Bürger schlugen auch verbesserte Verfahren vor, bei denen beispielsweise weniger Daten erfasst werden müssten oder die sich per technischer Kontaktdaten-App realisieren ließen.

In der Tat haben wir uns auch mit Alternativen beschäftigt und auch Meldungen zu Sicherheitsproblemen bei Datenbanken ausgewertet, bei denen Dienstleister von sehr vielen Einrichtungen zentral die Kontaktdaten speicherten – und leider nicht ausreichend gegen unberechtigte Zugriffe sicherten. In dem Fall hätte man nicht nur feststellen können, wer in welchem Restaurant essen gegangen ist, sondern man hätte auch auswerten können, wer mit wem dort war. Besonders bei Berufsgruppen wie Anwälten und Journalisten sind dies aber sehr sensible Daten, auf die nicht unbefugt zugegriffen werden darf. Von solchen technischen Lösungen haben wir abgeraten. Bessere Realisierungen arbeiten mit verschlüsselter Speicherung der Kontaktdaten auf eine Weise, dass noch nicht einmal der Betreiber der Einrichtung beim Vorzeigen den Namen erfährt und auch später nicht auf den Klartext der Daten zugreifen kann. Dennoch ist gewährleistet, dass im Infektionsfall ein Gesundheitsamt die Kontaktnachverfolgung durchführen kann. Allerdings besteht bei dieser datensparsameren Realisierung Anpassungsbedarf der rechtlichen Regelungen zur Kontaktdatensammlung.

Was ist zu tun?

Bei künftigen Anpassungen der Regelungen zu Coronamaßnahmen sollten die Formulierungen zumindest Raum für datensparsamere und risikoärmere Lösungen lassen. Außerdem wäre es wünschenswert, wenn die Regierung verstärkt datenschutzkonforme Praxishilfen gäbe, denn offensichtlich hat nicht jeder Verantwortliche den Weg zu unseren Informationen gefunden.

5.4 Interessante Einzelfälle

5.4.1 Coronamaßnahme Kontaktdatensammlung: Schludrigkeiten und Missbrauch

Die Verpflichtung zur Kontaktdatenerhebung ergibt sich aus der jeweils aktuellen Fassung der Landesverordnung zur Bekämpfung des Coronavirus SARS-CoV-2 des Landes-Schleswig-Holstein (SARS-CoV-2-BekämpfV) (siehe Tz. 5.3). Diese Verpflichtung gilt insbesondere für Gaststätten.

Diese Art der Erhebung personenbezogener Daten stellte ein Novum dar. Es zeigte sich anhand der zahlreichen Anfragen beim ULD, dass sowohl seitens der Verantwortlichen als auch bei den Gästen bzw. den Kundinnen und Kunden Unklarheiten hinsichtlich der Umsetzung der datenschutzrechtlichen Bestimmungen bei der Kontaktdatenerhebung vorlagen. Das ULD informierte daher ausführlich zum Datenschutz bei der Kontaktdatenerhebung:

https://www.datenschutzzentrum.de/artikel/1332-Infektionsschutz-Regelung-Datenschutz-bei-der-Erhebung-von-Kontaktdaten-Die-Landesbeauftragte-fuer-Datenschutz-Schleswig-Holstein-informiert.html

Kurzlink: *https://uldsh.de/tb39-5-41*

Hinsichtlich der Kontaktdatenerhebung bei Betrieben, die zur Erhebung verpflichtet waren, erreichte das ULD eine Vielzahl von Beschwerden.

1. Verstoß: Offen einsehbare Listen

Als häufigster Verstoß wurde die Kontaktdatenerhebung mittels einer offen einsehbaren Liste angezeigt. In diesen Fällen erfolgte die Erhebung in der Form, dass den Gästen eine Liste ausgehändigt wurde, in die die Kontaktdaten eingetragen werden sollten. Hierbei konnten die Gäste sämtliche zuvor eingetragenen Daten anderer Gäste einsehen. Diese Art der Erhebung stellt einen Verstoß gegen Artikel 24 und Artikel 32 DSGVO dar, wonach der Verantwortliche mittels geeigneter Maßnahmen gewährleisten muss, dass unbefugte Dritte von den erhobenen Daten keine Kenntnis erlangen.

2. Verstoß: Übermäßige Kontaktdatenerhebung

Weiterhin wurde beim ULD angezeigt, dass seitens der Verantwortlichen unzulässig Daten erhoben wurden. Hierbei handelte es sich insbesondere um das Geburtsdatum. In der SARS-CoV-2-BekämpfV wird klar festgelegt, welche Daten zu erheben sind. Dies sind Vor- und Nachname und Anschrift sowie, soweit vorhanden, Telefonnummer oder E-Mail-Adresse. Darüber hinaus dürfen keine weiteren Daten erhoben werden, da für diese Erhebung keine Rechtsgrundlage vorliegt und hierdurch ein Verstoß gegen den Grundsatz der Datenminimierung vorliegt.

3. Verstoß: Nutzung der Daten zu anderen Zwecken

Eine weitere missbräuchliche Verwendung der erhobenen Kontaktdaten stellte die Nutzung der Daten zu anderen Zwecken dar. Die Kontaktdaten sollen erhoben werden, um sie im Bedarfsfall an die zuständige Behörde zu übermitteln, sofern dies zum Zwecke der Nachverfolgung von möglichen Infektionswegen erforderlich ist. Eine anderweitige Verwendung ist unzulässig. Dem ULD wurde etwa angezeigt, dass die erhobenen Daten seitens des Verantwortlichen verwendet werden sollten, um diese in die Kundendatenbank einzupflegen oder um diese zur Zustellung von Werbung zu nutzen. Auch für diese Art der Verarbeitung lag keine Rechtsgrundlage vor.

Aufgrund der Vielzahl der gemeldeten Verstöße und der Neuartigkeit der Kontaktdatenerhebung haben wir zumeist Hinweise an die Verantwortlichen erteilt, um so eine schnelle Verhaltensänderung zu erwirken. Bei herausragenden Verstößen wurden aufsichtsbehördliche Verfahren eröffnet. Hierzu gehörte das Verwenden der erhobenen Telefonnummern, um eine WhatsApp-Gruppe zu erstellen, in der Marketingaktionen des eigenen Restaurants beworben werden sollten, sowie die Weitergabe einer erhobenen Handynummer an eine Mitarbeiterin, damit diese ein klärendes Telefonat mit einem Gast hinsichtlich einer erfolgten Kritik an ihrer Person führen konnte.

5.4.2 Coronamaßnahme Kontaktdatensammlung – anfangs nicht beim Friseur

Im Zuge der Maßnahmen zur Bekämpfung des Coronavirus wurde für bestimmte Betriebe eine verpflichtende Erhebung der Kontaktdaten der Kunden bzw. der Gäste zur Nachverfolgung von Infektionsketten im Zusammenhang mit COVID-19 eingeführt (siehe Tz. 5.3 sowie Tz. 5.4.1).

Uns erreichte eine Vielzahl an Beschwerden hinsichtlich der Kontaktdatenerhebung durch Friseurbetriebe. Dies war Anlass für eine Prüfung der Rechtmäßigkeit der Kontaktdatenerhebung durch Friseurbetriebe.

Art. 6 Abs. 1 Buchst. c DSGVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachfolgenden Bedingungen erfüllt ist:

[…]

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn hierfür eine Rechtsgrundlage vorliegt. Im Fall der Kontaktdatenerhebung ergibt sich diese allein aus Art. 6 Abs. 1 Buchst. c DSGVO. Die Pflicht zur Erhebung der Kontaktdaten ergibt sich aus der jeweils gültigen Landesverordnung zur Bekämpfung des Coronavirus SARS-CoV-2 des Landes-Schleswig-Holstein (SARS-CoV-2-BekämpfV). In der Landesverordnung wird festgelegt, welche Betriebe verpflichtend Kontaktdaten zu erheben haben. In dieser Regelung fanden sich bis 29.11.2020 zwar allgemeine Regelungen für Friseurbetriebe; diese sahen jedoch keine verpflichtende Kontaktdatenerhebung für Friseurbetriebe vor.

Im Ergebnis lag für die Kontaktdatenerhebung durch Friseurbetriebe zur Nachverfolgung von Infektionsketten im Zusammenhang mit COVID-19 keine Rechtsgrundlage vor. Eine Erhebung der Kontaktdaten war demnach nicht rechtmäßig, sodass die Kontaktdatenerhebung im Zusammenhang mit COVID-19 durch Friseurbetriebe zu unterlassen war und in diesem Zusammenhang erhobene Daten zu löschen waren.

Um das Ergebnis der Prüfung auf schnellstem Weg den Friseurbetrieben mitzuteilen und künftige Verstöße zu vermeiden, haben wir ein Informationsschreiben erstellt und den Friseurbetrieben über die zuständige Kreishandwerkerschaft Nordfriesland-Süd verteilt. Erst danach entschloss sich der Gesetzgeber, mit der Neufassung der SARS-CoV-2-BekämpfV, die am 30.11.2020 in Kraft trat, nunmehr doch eine Kontaktdatenerhebung für „Dienstleistungen mit Körperkontakt“ und damit auch für Friseurbetriebe einzuführen.

Überraschende Kehrtwende: Nun gab es plötzlich eine Rechtsgrundlage, und zum 30.11.2020 – nachdem in den zahlreichen vorherigen Fassungen seit dem 05.06.2020 davon nicht die Rede gewesen war – hatte sich die Rechtslage von einem Verbot einer Kontaktdatenerhebung zu einer Verpflichtung gewandelt. Als Aufsichtsbehörde können wir nur die uns bekannte, veröffentlichte Rechtslage heranziehen – über eine geplante Änderung hatte man uns im Übrigen auch nicht informiert.

Die Informationen zur Kontaktdatenerhebung bei Friseurbetrieben sind hier verfügbar:

https://www.datenschutzzentrum.de/artikel/1346-.html

Kurzlink: *https://uldsh.de/tb39-5-42*

Was ist zu tun?

Wünschenswert wäre es, wenn wir als zuständige Datenschutzaufsichtsbehörde schneller Informationen über den Datenschutz betreffende geplante Änderungen der Rechtslage in Bezug auf Coronamaßnahmen erhielten.

5.4.3 Erhebung von Gesundheitsdaten von Vereinsmitgliedern als Coronamaßnahme

Nachdem die Anzahl der Infektionen mit dem Coronavirus im Sommer sank, boten die Vereine ihren Mitgliedern die Wiederaufnahme ihrer Aktivitäten an. In einzelnen hierzu eingereichten Anfragen berichteten Betroffene von Wiedereinstiegsbögen ihrer Vereine, auf denen sie mit Fragen zu ihrem Gesundheitszustand konfrontiert wurden.

Die von den in den Bereichen Sport und Kultur tätigen Vereinen gestellten Fragen bezogen sich beispielsweise auf die mögliche Zugehörigkeit zu einer Risikogruppe aufgrund von Vorerkrankungen wie Diabetes, Krebs oder einer chronischen Leber- oder Lungenerkrankung. In einem anderen Verein wurden die Mitglieder um Angaben zur aktuellen Symptomatik wie beispielsweise Durchfall, Halsschmerzen oder Fieber gebeten. Die Vereine stellten ihren Mitgliedern in diesem Zusammenhang in Aussicht, dass diese im Falle einer Verweigerung der Auskunft an Aktivitäten des Vereins nicht mehr teilnehmen dürften.

Da sich die zum Zeitpunkt der Anfragen geltende Landesverordnung zur Bekämpfung des Coronavirus SARS-CoV-2 lediglich auf die Erhebung von Kontaktdaten beschränkte und eine solche weiter gehende Erhebung nicht vorsah, bestand keine rechtliche Verpflichtung zur Erhebung dieser Gesundheitsdaten, und die Erhebung konnte auch nicht auf Art. 6 Abs. 1 Buchst. c DSGVO gestützt werden. Die erbetenen Gesundheitsdaten unterliegen darüber hinaus einem besonderen Schutz und dürften nur unter den Voraussetzungen des Art. 9 Abs. 2 DSGVO verarbeitet werden.

Des Weiteren konnte die Erhebung auch nicht auf Grundlage einer Einwilligung erfolgen, da die Vereine den betroffenen Mitgliedern im Falle einer Verweigerung der Auskunft den Ausschluss von Vereinsaktivitäten in Aussicht stellten und somit nicht von der für eine wirksame Einwilligung erforderlichen Freiwilligkeit ausgegangen werden konnte.

Die erläuterte Problematik beschränkte sich auf Einzelanfragen betroffener Mitglieder, die lediglich um eine rechtliche Bewertung baten und die Beendigung der Erhebungspraxis jeweils vereinsintern besprechen wollten. Die datenschutzrechtlichen Bedenken gegen die Verwendung der Wiedereinstiegsbögen wurde ihnen jeweils entsprechend mitgeteilt, von weiteren Maßnahmen gegenüber den Vereinen wurde auf Bitte der betroffenen Mitglieder zunächst abgesehen.

5.4.4 Weitergabe von Daten aus einem Kundenbindungssystem

Viele Einzelhandelsunternehmen nutzen zur Kundenbindung ein Kundenkartensystem. Im Rahmen des Antrags auf Ausgabe einer Kundenkarte werden hier zunächst personenbezogene Daten wie Name, Adressdaten, Geburtsdatum und bei gleichzeitiger Nutzung als Zahlungsmittel auch Zahlungsdaten erhoben; diese werden im Verlauf der Nutzung der Karte mit den hieraus erworbenen Daten zum Einkaufsverhalten angereichert. Als Vorteile für die Kunden zur Teilnahme am Kundenkartensystem werden zumeist Rabatte auf Einkäufe, die Teilnahme an Sonderaktionen und weitere Vergünstigungen angeboten.

Die Inhaber von Kundenkarten eines derartigen Systems wurden im Laufe des Jahres über die

bevorstehende Schließung des ausgebenden Unternehmens informiert. Zugleich wurden sie darüber informiert, dass mit ihrer stillschweigenden Zustimmung ihre Daten an nicht näher bezeichnete Nachfolgefirmen, die die Räumlichkeiten zukünftig nutzen würden, weitergegeben würden; die Einwilligung erfolge auf freiwilliger Basis. Sollten die Kunden mit der Weitergabe ihrer Daten nicht einverstanden sein, wurden sie gebeten, einen entsprechend ausgedruckten Widerruf schnellstmöglich an das Unternehmen zurückzusenden. Als gesetzliche Grundlage verwies der Verantwortliche darauf, dass „die persönlichen Daten Ihrer Person unter Beachtung des Landesdatenschutzgesetzes (LDSG) erhoben, verarbeitet und genutzt werden".

Die geplante Weitergabe der personenbezogenen Daten wurde dem ULD durch mehrere Beschwerden bekannt.

Der Verantwortliche wurde im Rahmen eines aufsichtsbehördlichen Verfahrens zunächst darauf hingewiesen, dass die gesetzliche Grundlage für die Verarbeitung der personenbezogenen Daten im vorliegenden Fall die Datenschutz-Grundverordnung ist. Da das Landesdatenschutzgesetz lediglich für die Verarbeitung personenbezogener Daten bei öffentlichen Stellen des Landes Schleswig-Holstein gilt, war es im vorliegenden Fall nicht anzuwenden.

Die Weitergabe der personenbezogenen Daten sollte laut dem Kundenanschreiben auf Grundlage einer Einwilligung erfolgen, sodass in einer rechtlichen Würdigung ausgeführt wurde, dass eine Einwilligung einer betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung ist, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Das Anschreiben erfüllte die Voraussetzungen für eine wirksame Einwilligung bereits aus dem Grunde nicht, weil diese nicht durch eine bestätigende Handlung, sondern stillschweigend erfolgen sollte und nur durch einen Widerspruch abgewendet werden konnte. Die im Anschreiben enthaltenen Ausführungen zur Weitergabe der personenbezogenen Daten reichten zudem nicht aus, um den Anforderungen an eine informierte Einwilligung zu genügen.

Ergänzend ist anzumerken, dass der Verantwortliche, wenn die Verarbeitung auf einer Einwilligung beruht, nachweisen können muss, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Auch dies wäre durch das geplante Vorgehen nicht gegeben gewesen.

Nach Darlegung der Rechtsgrundlagen teilte der Verantwortliche mit, auf die Weitergabe der Kundendaten zu verzichten, diese unmittelbar nach der Schließung zu löschen und die betroffenen Personen hierüber zu informieren.

5.4.5 Geodaten bei Starkregenereignissen

Immer häufiger kommt es auch in Deutschland zu Überschwemmungen durch Starkregenereignisse, die zu erheblichen Sachschäden führen und bereits auch Menschenleben gefordert haben. Von Starkregen wird gesprochen, wenn innerhalb kurzer Zeit außergewöhnlich große Mengen an Niederschlag auftreten. Für die Entwicklung eines Starkregen-Risikomanagements ist die Gefährdungseinschätzung besonders für Orte in der Stadt eine wichtige Grundlage. Das Forschungsverbundprojekt „I2-Optimierung" der Fachgruppe Städtebau und Stadtentwicklung Technische Hochschule Lübeck beschäftigt sich mit diesem Thema.

In dem Projekt soll eine nutzungsspezifische Kategorisierung von Geodaten erfolgen, die das ULD zur Beurteilung der datenschutzrechtlichen Relevanz begleitet. Geodaten sind digitale Informationen, denen auf der Erdoberfläche eine bestimmte räumliche Lage, also ein Ort, zugewiesen werden kann.

Zur Beurteilung der datenschutzrechtlichen Relevanz von Geodaten wird ein Ampelverfahren genutzt. Geodaten werden als „grüne", „gelbe" und „rote" Daten auf der Grundlage eines standardisierten Fragenkatalogs von den geodatenhaltenden Stellen erfasst. Dabei ermöglicht der Fragenkatalog die Zuordnung der Geodaten zu einer Kategorie.

Anders als bei der „grünen" Kategorie sind die „gelben" und „roten" Geodaten aus Datenschutzsicht mit mehr Vorsicht zu behandeln. In dem

Projekt sollen den geodatenhaltenden Stellen Möglichkeiten zur Verwendung oder Offenlegung aufgezeigt werden, indem beispielsweise Maßstabsbeschränkungen zur Reduzierung des Datenschutzrisikos vorgenommen werden.

Was ist zu tun?

Auch Geodaten „verraten“ oft personenbezogene Daten. Werden Geodaten, die einen Personenbezug aufweisen, verarbeitet und z. B. veröffentlicht, ist die DSGVO anwendbar. Die Möglichkeit, dass damit Rechte und Freiheiten von natürlichen Personen betroffen sind, nimmt zu, je mehr diese und andere Daten öffentlich verfügbar werden und miteinander verknüpft werden können. Darum ist im Einzelfall genau zu prüfen, unter welchen Bedingungen Geodaten der Öffentlichkeit zugänglich gemacht werden können.

5.4.6 Nutzung von „dienstlichen“ Messengergruppen des Arbeitgebers über private Endgeräte

Zahlreiche Beschäftigte werden von ihren Kolleginnen und Kollegen oder ihren Vorgesetzten mit der Frage konfrontiert, wie ihre private Handynummer laute und ob sie nicht in die häufig bereits vorhandene Messengergruppe aufgenommen werden möchten. Diese würde genutzt werden, um sich privat oder – falls erforderlich – auch mal kurzfristig dienstlich austauschen zu können. Was von den Betroffenen anfangs zunächst als hilfreich und unproblematisch empfunden wird, kann sich allerdings schnell zu einem Problem entwickeln.

In verschiedenen hierzu eingereichten Beschwerden berichteten Betroffene, dass entsprechende Gruppen regelmäßig genutzt werden, um sich kurzfristig krankzumelden und eine Vertretung zu organisieren. Zum Teil würden hierbei allerdings auch Nachfragen zum Grund der Erkrankung erfolgen und Dienstpläne erstellt sowie übermittelt werden. Bei der Erstellung von Dienstplänen könnten hierbei leider nur Wünsche von Mitarbeiterinnen und Mitarbeitern berücksichtigt werden, die auch Mitglieder in der Messengergruppe seien, sodass eine Ablehnung der Teilnahme an der Gruppe negative Folgen habe. Darüber hinaus wurde die permanente Erreichbarkeit von den Betroffenen als Belastung empfunden und führte in einem Fall zum Wechsel der privaten Handyrufnummer. In einer anderen Beschwerde beklagte sich eine ehemalige Beschäftigte darüber, dass ihre bisherige Vorgesetzte die Messengergruppe genutzt habe, um den übrigen Kolleginnen und Kollegen den Hintergrund der erfolgten Beendigung ihres Arbeitsverhältnisses zu erläutern.

In den hierzu durchgeführten Verfahren wurden die Unternehmen zunächst darauf hingewiesen, dass es grundsätzlich Aufgabe des Arbeitgebers sei, den Beschäftigten die erforderlichen Arbeitsmittel zur Verfügung zu stellen. Eine Auslagerung der Datenverarbeitung auf private Endgeräte, die zusätzlich dazu führe, dass private Rufnummern und Accounts der Beschäftigten mitverarbeitet werden, sei grundsätzlich nicht erforderlich und statthaft.

Bei der Nutzung entsprechender Gruppen zur Übermittlung oder Offenlegung personenbezogener Daten zu dienstlichen Zwecken ist das betroffene Unternehmen für die Gewährleistung eines angemessenen Schutzniveaus verantwortlich. Hierbei sind vom verantwortlichen Unternehmen u. a. geeignete Maßnahmen zu treffen, um zu gewährleisten, dass Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Diese erforderlichen Maßnahmen können Verantwortliche auf den betroffenen privaten Endgeräten in der Regel nicht gewährleisten, da auf diesen auch technische Schwachstellen durch veraltete Systeme oder inaktuelle Sicherheitsupdates vorliegen können und für die Gewährleistung eines angemessenen Schutzniveaus die Kontrolle der privaten Endgeräte der Beschäftigten erforderlich wäre.

In den durchgeführten Verfahren berichteten Geschäftsführer und Datenschutzbeauftragte zum Teil von eigenmächtigem Handeln der unteren

Führungsebenen, die hier gegen entsprechende Unternehmensrichtlinien verstoßen würden. Die betroffenen Unternehmen haben die betreffenden Mitarbeiterinnen und Mitarbeiter in Führungsverantwortung teilweise gerügt, alle Beschäftigten auf das Verbot der Nutzung privater Endgeräte für dienstliche Zwecke hingewiesen und die Löschung der vorhandenen Messengergruppen veranlasst. Darüber hinaus wurden in einem Unternehmen die Arbeitsverträge um eine entsprechend klarstellende Formulierung ergänzt.

Unabhängig von der Nutzung der Messengergruppen wurde die beschriebene Mitteilung der Hintergründe einer erfolgten Beendigung eines Arbeitsverhältnisses gegenüber den übrigen Kolleginnen und Kollegen zum Anlass genommen, das betreffende Unternehmen hierzu zu verwarnen.

Was ist zu tun?

Eine dienstliche Nutzung von privaten Endgeräten sollte grundsätzlich unterbunden und gegenüber den Beschäftigten transparent kommuniziert werden. Hierbei hat der Arbeitgeber seine Beschäftigten mit den erforderlichen Endgeräten auszustatten, sodass diese nicht mangels Ausstattung gezwungen sind, auf private Endgeräte auszuweichen. Die Einhaltung von getroffenen Regelungen ist regelmäßig zu überprüfen.

5.4.7 Weitergabe von Informationen über Erkrankungen eines Beschäftigten an den neuen Arbeitgeber

Im Frühjahr 2020 ging beim ULD eine Beschwerde ein, in der ein Beschäftigter beklagte, sein zukünftiger neuer Arbeitgeber sei von seinem bisherigen Arbeitgeber über eine dort abgegebene Arbeitsunfähigkeitsbescheinigung verbunden mit dem Kommentar informiert worden, dass er ein Krankmacher sei.

Nach § 26 Abs. 1 BDSG dürfen personenbezogene Daten von Beschäftigten nur für den Zweck des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung für dessen Durchführung oder Beendigung erforderlich ist. Die Verpflichtung zur Vorlage einer Arbeitsunfähigkeitsbescheinigung ergibt sich aus § 5 Entgeltfortzahlungsgesetz, dient dem Nachweis der Arbeitsunfähigkeit und zum Zweck der Prüfung der Entgeltfortzahlung.

Die auf einer Arbeitsunfähigkeitsbescheinigung enthaltenen Daten sind im Sinne des Artikels 9 DSGVO besonders sensibel, da aus diesen u. a. auch erkennbar ist, welche Ärztin oder welcher Arzt die oder den Beschäftigten behandelt und über welche Qualifikation diese Ärztin bzw. dieser Arzt verfügt, sodass der Arbeitgeber anhand dieser Informationen mögliche Krankheitsbilder grob eingrenzen kann.

BAG-Urteil vom 12.09.2006 – 9 AZR 271/06

Soweit Gesundheitsdaten in die Personalakte aufgenommen werden dürfen, ist der Arbeitgeber verpflichtet, die Daten in besonderer Weise aufzubewahren. Die zur Personalakte genommenen Gesundheitsdaten sind vor unbefugter zufälliger Kenntnisnahme durch Einschränkung des Kreises der Informationsberechtigten zu schützen. Jeder Mitarbeiter darf nur auf solche Daten zugreifen können, die er zur Erfüllung seiner Aufgaben tatsächlich benötigt.

Der verantwortliche Arbeitgeber hat bei der Verarbeitung von Personal- und Gesundheitsdaten seiner Beschäftigten sicherzustellen, dass die Sicherheit der Verarbeitung und die Vertraulichkeit der Informationen gewährleistet sind. Hierzu zählt u. a. ein entsprechendes Berechtigungskonzept,

das den Zugriff auf vertrauliche Personal- und Gesundheitsdaten einschränkt. Des Weiteren sind Maßnahmen zu treffen, die einen unbefugten Zugriff oder eine Offenlegung von personenbezogenen Daten der Mitarbeiter gegenüber Unberechtigten verhindern.

Die vorgenommene Übermittlung von Informationen über eine Arbeitsunfähigkeitsbescheinigung an den neuen Arbeitgeber war weder für die Durchführung noch für die Beendigung des Beschäftigtenverhältnisses erforderlich, beinhaltete eine unzulässige Zweckänderung und war somit datenschutzrechtlich unzulässig.

Da der Betroffene auf Nachfrage allerdings mitteilte, dass er von seinem neuen Arbeitgeber über den Sachverhalt nur mündlich informiert worden sei und dieser ihm auch auf Nachfrage keine Belege hierfür zur Verfügung stelle, wurde dem bisherigen Arbeitgeber gegenüber lediglich ein Hinweis auf einen vermeintlichen Verstoß erteilt.

5.5 Datenpannen in der Wirtschaft

5.5.1 Besondere Zeiten: Datenpannen im Lockdown

Als Coronamaßnahme mussten in diesem Jahr einige Branchen aufgrund der ergangenen Landesverordnung ihren aktiven Geschäfts- oder Vereinsbetrieb vorübergehend einstellen oder einschränken, Auswirkungen der Pandemie ergaben sich in unterschiedlichem Maße für nahezu alle Verantwortlichen.

Um ihre Kundinnen und Kunden oder Mitglieder über Schließungen, Wiedereröffnungen, geänderte Öffnungszeiten oder weitere Maßnahmen zu benachrichtigen, wählten viele Verantwortliche eine Zusendung von Informationen per E-Mail. Hier kam es zu einer Vielzahl von Versendungen mit offenem E-Mail-Verteiler und somit zur unrechtmäßigen Offenlegung von personenbezogenen Daten, denn die Empfänger erfuhren auf diese Weise unbefugt Namen und E-Mail-Adressen anderer Personen.

In einem weiteren Fall erfolgte zwar der Versand eines Informationsschreibens per E-Mail korrekt, allerdings war der E-Mail anstatt eines nicht personalisierten Schreibens ein zuvor erstellter Serienbrief angehängt, aus dem sich sämtliche Namen und Anschriften derjenigen Personen ergaben, denen das Schreiben auf dem Postweg zugestellt wurde. Eine Kontrolle durch Aufrufen und Prüfen der angehängten Datei vor dem Absenden hätte als organisatorische Maßnahme mit wenig Aufwand die unbefugte Offenlegung der personenbezogenen Daten abwenden können.

Bei vielen Verantwortlichen wurde die Anzahl der im Unternehmen vor Ort tätigen Beschäftigten reduziert und die Tätigkeiten, soweit möglich, von zu Hause aus im sogenannten Homeoffice (siehe auch Tz. 6.3.3) ausgeübt. Da die bisherigen Infrastrukturen nicht umfassend zur Verfügung standen, waren die üblichen Arbeitsabläufe teilweise gestört. Wege, sich diesbezüglich zu behelfen, standen nicht immer im Einklang mit der Datenschutz-Grundverordnung und führten somit zu weiteren Verletzungen des Schutzes personenbezogener Daten.

So stellte ein Verantwortlicher bei der Prüfung von Unregelmäßigkeiten im Bereich der E-Mail-Verarbeitung fest, dass mittels eines unrechtmäßig installierten Programms zur Fernnutzung von Computern von einem externen Computer Zugriff auf den Dienstcomputer einer Filiale genommen wurde. Die weiteren Ermittlungen ergaben, dass sich ein Beschäftigter die Freiheit genommen hatte, ohne Wissen seines Arbeitgebers sich selbst unerlaubt ins Homeoffice zu „versetzen“. Um von zu Hause aus Kunden-E-Mails beantworten zu können, hatte er in diesem Zusammenhang eine Weiterleitung der auf den dienstlichen E-Mail-Account eingehenden Nachrichten an seine eigene private E-Mail-Adresse veranlasst.

Zu einer besonders umfangreichen Offenlegung von personenbezogenen Daten, die wohl auch in der geänderten Arbeitssituation in Zusammenhang mit den durch den Arbeitgeber getroffenen Maßnahmen zum Schutz der Beschäftigten begründet lag, kam es durch eine fehlerhafte Nutzung eines Transferlaufwerks. Um einem derzeit aus dem Homeoffice arbeitenden Beschäftigten zur Lösung von technischen Problemen Zugriff auf eine Mitarbeiterstatistik zu gewähren, wurde ihm diese auf

einem Transferlaufwerk zur Verfügung gestellt – jedoch hatten außer ihm darauf auch sämtliche zu dieser Zeit im System angemeldeten Beschäftigten Zugriff. Der Verantwortliche stellte dar, dass dem Personalbereich zum sicheren Datentransfer von vertraulichen Daten entsprechende IT-Lösungen zur Verfügung stünden; durch einen Arbeitsfehler sei es dennoch zu der beschriebenen Verletzung des Schutzes personenbezogener Daten gekommen.

Was ist zu tun?

Besondere Zeiten bedürfen besonderer Lösungen, diese müssen jedoch dennoch den Vorgaben der Datenschutz-Grundverordnung entsprechen.

5.5.2 Gemeldete Datenpannen: Offenlegung personenbezogener Daten durch falsche Berechtigungen

Dem Erstellen eines Berechtigungskonzepts sowie dessen Pflege und korrekter Verwaltung kommt als technischer und organisatorischer Maßnahme zum Schutz personenbezogener Daten eine große Bedeutung zu. Je nach Komplexität und Dynamik sind teilweise häufige Anpassungen notwendig, bei denen es immer wieder zu Fehlern kommt.

Bei den diesbezüglich gemeldeten Verletzungen des Schutzes personenbezogener Daten handelte es sich zumeist um die Erteilung fehlerhafter Berechtigungen für Beschäftigte, die auf diese Weise Zugriff auf die personenbezogenen Daten ihrer Kolleginnen und Kollegen erhielten; in einem Fall konnte Zugriff auf Ordner des Betriebsrats genommen werden.

Als Grund für die Einrichtung der fehlerhaften Berechtigung wurde in allen Fällen ein **menschlicher Fehler** der mit der Aufgabe betrauten Beschäftigten genannt. Einige Verantwortliche zeigten sich überrascht davon, dass diese Begründung für eine abschließende Bewertung des Vorfalls **nicht als ausreichend betrachtet** wurde. Da jedoch durch den Verantwortlichen geeignete technische und organisatorische Maßnahmen zu treffen sind, die den Schutz der personenbezogenen Daten gewährleisten, ist eine genauere Betrachtung erforderlich: Wie kam es zu dem menschlichen Fehler? Hier wurde den Verantwortlichen im Rahmen des aufsichtsbehördlichen Verfahrens die Gelegenheit gegeben, zu den zum Zeitpunkt des Vorfalles ergriffenen Maßnahmen (z. B. Prozesse, Arbeitsanweisungen, Ressourcen) Stellung zu nehmen. In verschiedenen Fällen wurde auf die Möglichkeit zur Stellungnahme verzichtet, jedoch angekündigt, das Rechtemanagement anlässlich der Verletzung des Schutzes personenbezogener Daten einer Revision zu unterziehen, teilweise unter Hinzuziehung von externen Fachkräften.

Eine Berechtigungsproblematik aus technischer Sicht ergab sich für einen Verantwortlichen bei der Nutzung eines Lohnportals. Der Personalbereich selbst lud hier die Steuerbescheinigungen der Beschäftigten auf das Portal hoch, die so Zugriff auf ihre Daten erhielten. In dem gemeldeten Sachverhalt wurde eine Bescheinigung unbemerkt irrtümlich in einem Format erstellt, das dazu führte, dass das Portal keine automatische Zuordnung der hochgeladenen Daten zu der passenden Person ausführen konnte. In der Folge wurde jedoch keine Fehlermeldung generiert, sondern die Steuerbescheinigung für sämtliche am Portal teilnehmenden Personen zur Einsichtnahme bereitgestellt. Als organisatorische Maßnahme zur Gewährleistung der Sicherheit der personenbezogenen Daten bestand für die mit der Verarbeitung betraute Beschäftigte die Anweisung, die korrekte Ausführung zu kontrollieren, was jedoch nicht erfolgte. Allerdings könnte hier auch in der technischen Funktionalität des Portals nachgebessert werden, denn eine Bereitstellung eines Dokuments für alle Beschäftigten sollte nicht der Standardfall sein.

Ebenfalls in Zusammenhang mit der Nutzung von Portalen standen Verletzungen des Schutzes personenbezogener Daten, die sich aus der fehlerhaften Vergabe von Zugangscodes ergaben. So beauftragte eine Baugenossenschaft einen

Dienstleister, die Kontaktdaten der Mieterinnen und Mieter über ein Portal abzufragen. Beim Druck der Anschreiben mit jeweils einem persönlichen Zugangscode wurden jedoch die Codes nicht korrekt übernommen. In der Folge erhielten alle Empfängerinnen und Empfänger denselben Zugangscode und konnten nach dem Einloggen die Daten derjenigen Mieterinnen und Mieter sehen, die bereits Änderungen vorgenommen hatten. Trotz einer stichprobenartigen manuellen Kontrolle vor dem Absenden war der Fehler nicht entdeckt worden.

Was ist zu tun?

In Zusammenhang mit getroffenen technischen Maßnahmen ist jeweils zu beachten, welche flankierenden organisatorischen Maßnahmen erforderlich sind, um einen angemessenen Schutz der personenbezogenen Daten zu gewährleisten.

5.5.3 Gemeldete Datenpannen: Diebstahl und Verlust von Hardware

Im Jahr 2020 gingen dem ULD mehrere Meldungen der Verletzung des Schutzes personenbezogener Daten zu, die den Diebstahl oder den Verlust von Hardware betrafen.

Die Art und Schwere der Vorfälle sowie der Grad der Fahrlässigkeit im Hinblick auf die zur Gewährleistung der Sicherheit der personenbezogenen Daten getroffenen Maßnahmen unterschieden sich hierbei stark. Aus technischer Sicht von Bedeutung war insbesondere, dass teilweise Datenträger mit personenbezogenen Daten nicht verschlüsselt wurden, obwohl diese den in der Regel hinreichend geschützten Bereich der Unternehmen verließen: So erfolgte in zwei Fällen der Versand von unverschlüsselten Datenträgern in einfachen Briefen. Der Verbleib eines USB-Sticks mit sensiblen Beschäftigtendaten blieb ungeklärt, da der Briefumschlag den Empfänger beschädigt und ohne den Datenträger erreichte (siehe auch Tz. 4.5.5), eine verloren geglaubte CD wurde zu einem späteren Zeitpunkt wieder aufgefunden.

In einem weiteren Fall wurde dem ULD der Diebstahl einer unverschlüsselten Festplatte mit umfangreichen personenbezogenen Kunden- und Beschäftigtendaten aus einem Back-up gemeldet. Die Festplatte war in einem Raum aufbewahrt worden, zu dem zwar nur ein begrenzter Personenkreis Zugang hatte, weitere physische Maßnahmen (z. B. Lagerung in einem abschließbaren Sicherheitsschrank) wurden jedoch nicht getroffen. Die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der personenbezogenen Daten reichten nicht aus.

Die Relevanz der organisatorischen Maßnahmen sowie die Notwendigkeit, diese konsequent anzuwenden, zeigte sich auch bei Meldungen, die in Zusammenhang mit der Bereitstellung von Hardware an Beschäftigte standen.

So wurde im Zuge der Prüfung eines Diebstahls eines unverschlüsselten Tablets durch eine Befragung des Beschäftigten festgestellt, dass hierauf entgegen der Annahme des Verantwortlichen personenbezogene Daten gespeichert worden waren, obwohl das Tablet hierfür nicht vorgesehen war. Der Umfang der Nutzung der zur Verfügung gestellten Hardware ist als organisatorische Maßnahme konkret festzulegen, entsprechend zu kommunizieren und auch in datenschutzrechtlichen Schulungen zu thematisieren.

Dass sich jedoch auch bei umfassenden organisatorischen Maßnahmen durch den Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten nicht vollständig ausschließen lässt, zeigte ein Vorfall, der sich auf ein **bewusstes Fehlverhalten eines Beschäftigten** zurückführen ließ. Entgegen der ihm erteilten detaillierten Anweisungen führte dieser neben seinem verschlüsselten Notebook auch einen unverschlüsselten USB-Stick mit darauf gespeicherten personenbezogenen Daten im Urlaub mit sich; beides wurde aus einem Pkw entwendet. Das Unternehmen nahm den Vorfall

zum Anlass, die Sicherheit durch die technische Maßnahme zu erhöhen, das Speichern von Daten auf externen Datenträgern grundsätzlich zu deaktivieren. Das Reaktivieren dieser Funktion im berechtigten Einzelfall erfordert nun das Durchlaufen eines Genehmigungsprozesses, in dem die Ausnahme nachvollziehbar begründet werden muss.

Unter Abwägung insbesondere der Art, Schwere und Dauer des jeweiligen Verstoßes, dem Grad der Fahrlässigkeit und unter Berücksichtigung der ergriffenen Maßnahmen zur Minderung des eventuell entstandenen Schadens wurden gegenüber den Verantwortlichen Hinweise, Verwarnungen sowie auf die Zukunft gerichtete Warnungen ausgesprochen.

5.6 Videoüberwachung

Schon seit vielen Jahren ist Videoüberwachung ein Dauerbrenner unter den Beschwerden. Im Berichtszeitraum stiegen die Fallzahlen weiter an. Im Vergleich zu **2018** haben sich **die Beschwerden im Jahr 2020 nahezu verdoppelt**. Der Schwerpunkt lag dabei eindeutig auf Prüfungen von Videoüberwachungsanlagen von nichtöffentlichen Stellen, die durch Beschwerden bekannt geworden sind.

Nach wie vor gibt es zahlreiche Beschwerden über Videoüberwachung im Nachbarschaftskontext. Die Videoüberwachung hat aber bereits sämtliche Lebensbereiche durchdrungen – sie ist immer häufiger in Restaurants, Kliniken, Vereinen, Bürogebäuden von Unternehmen, Mehrfamilienhäusern, Schulen, in der Heilpraktikerpraxis oder in der Bäckerei um die Ecke zu finden. Die vermeintliche Kamera des bösen Nachbarn entpuppt sich zwar manchmal als Infrarot-Tiervertreiber oder als harmloses Vogelhäuschen. In einigen wenigen Fällen ist aber schon zu Beginn des Verfahrens klar, dass ein erheblicher Verstoß gegen die Datenschutz-Grundverordnung vorliegt und manchmal sogar eine **Straftat** im Raum steht. Das ist regelmäßig **bei verdeckten Videoüberwachungen** der Fall.

Üblicherweise werden die Verantwortlichen im Rahmen ihrer Kooperationsbereitschaft gebeten, auf freiwilliger Basis zu der betriebenen Videoüberwachung Stellung zu nehmen. Sofern sich die Verantwortlichen nicht freiwillig zum Sachverhalt äußern, können sie nach Art. 58 Abs. 1 Buchst. a DSGVO zu einer Auskunft verpflichtet werden. Das ist oftmals notwendig, da wir für eine vollständige Bewertung, ob die Videoüberwachung zulässig ist oder nicht, auf bestimmte Angaben angewiesen sind. Allein im Bereich der Videoüberwachung wurden im Berichtszeitraum daher 23 Auskunftsanordnungen erlassen. Dies geschieht immer dann, wenn die Verantwortlichen nicht freiwillig zum Vorwurf Stellung beziehen. Die Zahl zeigt aber auch, dass ein Großteil der Verantwortlichen durchaus kooperationsbereit ist und auf freiwilliger Basis eine Stellungnahme zur Videoüberwachung abgibt.

Im Berichtszeitraum wurde die Videoüberwachung zudem in elf Fällen ganz oder teilweise untersagt. Bei einer Kooperationsbereitschaft der Verantwortlichen erreichen wir oftmals bereits durch konstruktive Hinweise eine Veränderung der Videoüberwachung, sodass Verstöße gegen die Datenschutz-Grundverordnung beseitigt werden.

Insgesamt ist festzustellen, dass im Vergleich zu der Vergangenheit häufiger formelle Verfahren eingeleitet werden und auch die Anzahl der erlassenen Verwaltungsakte in diesem Bereich zugenommen hat. In einigen Fällen befinden wir uns bereits im Vollzug dieser Verwaltungsakte durch die Androhung und Festsetzung von Zwangsgeldern.

Verdeckte Videoüberwachung kann eine Straftat sein!

Wer eine Videoüberwachungskamera versteckt, um heimlich Aufnahmen z. B. von Mitarbeiterinnen und Mitarbeitern, Kundinnen und Kunden oder sogar Patientinnen und Patienten zu erstellen, macht sich nach § 201a Strafgesetzbuch (StGB) unter Umständen strafbar. Wir raten daher ausdrücklich von solchen Überlegungen ab. Betroffene Personen können sich gern mit Hinweisen an uns wenden oder – da diese Tat nur auf Antrag verfolgt wird – direkt eine Strafanzeige bei der zuständigen Staatsanwaltschaft stellen.

5.6.1 Private Videoüberwachung zu Hause – wer schaut mit?

In den vergangenen Jahren gab es immer wieder Hinweise aus der Bevölkerung auf Webseiten, die Aufnahmen von ungesicherten Videoüberwachungskameras veröffentlichen. Derartige Webseiten haben häufig kein Impressum und werden in der Regel außerhalb der EU betrieben, wodurch sie weitgehend der Kontrolle von Datenschutzaufsichtsbehörden entzogen sind.

Die Kameras, deren Bilder auf solchen Webseiten veröffentlicht werden, weisen eine große Bandbreite auf. Zum Teil handelt es sich um Webcams, die z. B. eine Strandpromenade oder ein Hafenbecken zeigen. Hier scheint eine Veröffentlichung durchaus gewollt zu sein. Genauso sind aber private Überwachungskameras zu finden, die z. B. den Eingangsbereich vor einem Wohnhaus, eine Lagerhalle, einen privaten Parkplatz oder gar ein schlafendes Kind im Babybett überwachen. In diesen Fällen kann kaum davon ausgegangen werden, dass die Betreiber von solchen privaten Kameras eine Veröffentlichung der Aufnahmen oder des Livestreams beabsichtigen. Im Regelfall möchte man nicht, dass alle Welt sehen kann, wann man selbst oder die Familie das Haus verlässt. Für diese Kameras ist durchaus fraglich, ob der Betreiber weiß, dass diese Informationen frei zugänglich im Netz verfügbar sind.

Immer wieder kommt es vor, dass solche Webseitenbetreiber das Internet gezielt nach Kameras durchsuchen, die von den Anwendern ungeschützt und ohne Passwortsicherung mit dem offenen heimischen WLAN und darüber auch mit dem Internet verbunden werden.

Auf den Webseiten werden teilweise Angaben zu angeblichen Standorten der einzelnen Kameras veröffentlicht. Unsere Recherche hat ergeben, dass diese nicht immer mit dem wahren Standort übereinstimmen. Bei einigen Kameras besteht die Möglichkeit, über die Homepage die Kontrolle über die Kamera zu übernehmen. Dies ermöglicht zum Teil ein Heranzoomen oder Schwenken der Kamera. Bei einigen Kameras war es in unseren technischen Tests zudem möglich, die Konfiguration zu ändern.

Was ist zu tun?

Personen, die eine Videoüberwachung betreiben und keine Veröffentlichung der Aufnahmen wünschen, sollten unbedingt geeignete technische Maßnahmen ergreifen, um nicht ungewollt zum nächsten Realitystar des Internets zu werden. Verlassen Sie sich nicht auf die voreingestellte Konfiguration (Voreinstellungen) und ändern Sie in jedem Fall das Standardpasswort. Vermeiden Sie Angaben, die auf den genauen Standort der Kamera schließen lassen, z. B. GPS-Daten oder textliche Beschreibungen. Wenn möglich ändern Sie den Erkennungstext (Herstellertext) der Kamera, damit die Erfassung durch Gerätesuchmaschinen erschwert wird. Achten Sie darauf, dass Sichtwinkeländerungen und Zoomfunktionen sowie Aufnahmen und Wiedergabe von Aufnahmen nur von berechtigten Personen durchgeführt werden können.

5.6.2 Kfz-Kennzeichenerfassung beim Parken

Eine Vielzahl von Beschwerden gab es im Berichtszeitraum zu Kfz-Kennzeichenerfassungssystemen zum Zweck der Parkraumbewirtschaftung. Die Systeme funktionieren oftmals so, dass bei der Einfahrt zur Parkfläche das Kfz-Kennzeichen des Fahrzeugs erfasst und zusammen mit der Uhrzeit der Einfahrt gespeichert wird. Wenn der Parkvorgang beendet werden soll, gibt man an einem Automaten sein Kfz-Kennzeichen ein und bezahlt den für die Parkdauer berechneten Betrag. An der Ausfahrt des Parkbereichs befindet sich eine weitere Kamera, die das Kfz-Kennzeichen des ausfahrenden Fahrzeuges erfasst und abgleicht, ob für dieses Kennzeichen die Parkkosten bezahlt wurden. In dem Fall öffnet sich die Schranke und das Fahrzeug kann den Parkbereich verlassen.

Andere Systeme verzichten auf die Schranken an der Ein- und Ausfahrt. Das kann schnell dazu führen, dass die betroffenen Personen gar nicht bemerken, dass sie einen kostenpflichtigen Parkbereich befahren. Das Gleiche gilt für die Ausfahrt, da ein Verlassen des Parkplatzes möglich ist, auch wenn für das Parken nicht bezahlt wurde. Fehlt die Zahlung, ermittelt der Parkflächenbetreiber über das vorhandene Kfz-Kennzeichen die Daten des Fahrzeughalters und fordert diesen auf, das Parkentgelt sowie eine Vertragsstrafe zu zahlen. Diese ist häufig mehr als doppelt so hoch wie der eigentlich zu entrichtende Betrag.

Die Parkflächenbetreiber geben für die Verarbeitung der Kfz-Kennzeichen zwei Rechtsgrundlagen an. Zum einen ist die Erfassung der Kfz-Kennzeichen nach ihrer Ansicht zur Erfüllung des Vertrags zwischen der betroffenen Person und dem Parkflächenbetreiber erforderlich. Zum anderen führen die Betreiber ein berechtigtes Interesse an, um sich gegen möglichen Parkzeitenbetrug zu schützen. Es komme häufig vor, dass Tickets verloren gingen und dann die Tageshöchstparkdauer gezahlt werden müsse. Dies sei weder für die Kunden noch für die Parkflächenbetreiber von Vorteil. Kunden müssten dann oft ein vielfach höheres Entgelt entrichten, als eigentlich notwendig gewesen wäre. Fälle, in denen Kunden ihr Fahrzeug tagelang auf einer Parkfläche abstellen und anschließend behaupten, das Parkticket verloren zu haben, bedeuteten einen wirtschaftlichen Verlust für den Parkflächenbetreiber. Durch eine Kfz-Kennzeichenerfassung könnten beide Fälle verhindert werden, da sich die exakte Parkdauer feststellen lasse.

Ob derartige Systeme aus datenschutzrechtlicher Sicht zulässig sind, lässt sich nicht pauschal beantworten. Wie so oft kommt es auf den Einzelfall an. Damit der Betreiber einer solchen Kfz-Kennzeichenerfassung die schutzwürdigen Interessen der betroffenen Personen ausreichend wahrt, muss deutlich und transparent auf die Datenverarbeitung hingewiesen werden. Den Fahrzeugführern muss bewusst gemacht werden, dass sie einen kostenpflichtigen Parkplatz befahren und das Kfz-Kennzeichen zu diesem Zweck erfasst wird. Zudem ist das Kennzeichen nur für den erforderlichen Zeitraum zu speichern und muss gelöscht werden, sobald der Parkvorgang und die Bezahlung abgeschlossen sind. Das System darf auch nicht zur Erstellung von Bewegungsprofilen oder zur Erfassung von Arbeitszeiten zweckentfremdet werden.

Es gibt auch Konstellationen, in denen die Kfz-Kennzeichenerfassung nicht zulässig ist. Wenn beispielsweise in einer privaten Tiefgarage eines Mehrfamilienhauses ein Kfz-Kennzeichenerfassungssystem genutzt würde, um dafür zu sorgen, dass nur berechtigte Personen Zugang zu der Tiefgarage erhalten, dürfte dieses Vorhaben höchstens aufgrund der Einwilligung der jeweiligen Betroffenen zulässig sein. Eine Interessenabwägung würde in diesem Fall zugunsten der betroffenen Personen ausschlagen, da diese kaum verpflichtet werden dürften, ihr Kennzeichen anzugeben. Wirtschaftliche Verluste, die durch das Verlieren von Parktickets entstehen, können hier auch nicht entstehen, da in solchen Tiefgaragen oder Parkhäusern die Parkfläche in der Regel nicht in Minuten oder Stunden abgerechnet wird. Entschließen sich Parkflächenbetreiber oder auch z. B. Wohnungseigentümergemeinschaften dazu, das Befahren eines privaten Parkhauses durch eine Kfz-Kennzeichenerfassung zu ermöglichen, sollte dies auf freiwilliger Basis erfolgen. Das bedeutet auch, dass für diejenigen, die damit nicht einverstanden sind, zusätzlich alternative Optionen angeboten werden, beispielsweise die Ausgabe von Parkkarten.

5.6.3 Videoüberwachung im Schwimmbad

Im vergangenen Jahr fand eine umfangreiche Prüfung einer Videoüberwachung in einem Schwimmbad statt. Im Bereich des Solebeckens des Bades waren zwei Videoüberwachungskameras installiert. Eine Kamera war auf die Wasseroberfläche, die andere auf das Drehkreuz am Zugang zum Solebecken und den dahinter gelegenen Umkleidebereich gerichtet. Ab einer bestimmten Uhrzeit ist dieses Becken ohne Badebekleidung zu nutzen.

Die Videoüberwachung der Wasseroberfläche wurde mit dem Schutz lebenswichtiger Interessen begründet. Das Becken ist im Außenbereich der Therme nahe an einer Hausfassade gelegen und umzäunt, sodass es durch die Badaufsicht nicht durch einfache Sichtkontrollen eingesehen werden kann. Eine Übertragung der Videobilder findet auf einen Monitor statt, der sich im Raum der Badaufsicht befindet. Dieser Raum ist nur der diensthabenden Badaufsicht zugänglich, die wiederum per Diensthandy die weiteren Mitarbeiterinnen und Mitarbeiter der Badaufsicht zu den potenziellen Einsatzorten schickt, wenn auf dem Monitor eine Situation wahrgenommen wird, die ein Eingreifen erfordert. Die Videobilder werden nicht gespeichert. Die Videobeobachtung der Wasseroberfläche des Solebeckens soll dazu beitragen, Leib, Leben und körperliche Unversehrtheit der betroffenen Personen zu schützen. Der Verantwortliche konnte darlegen, dass diese Schutzgüter im Solebecken durch die tatsächlichen Umstände, wie u. a. den hohen Salzgehalt und die Wärme, besonders gefährdet sind. Da es sich vorliegend um eine Videoüberwachung zum Schutz von sehr hochrangigen Rechtsgütern handelt und zumindest keine Speicherung der Aufnahmen erfolgt, haben wir – außer der Verbesserung der Informationen für die betroffenen Personen – keine Maßnahmen gegen den Betrieb der Kamera ergriffen.

Die Videoüberwachung des Zugangs zum Solebecken und des dahinter gelegenen Umkleidebereiches stützte die verantwortliche Stelle auf ihr berechtigtes Interesse: Durch die Videoüberwachung solle verhindert werden, dass sich Badegäste Zutritt zum Solebecken verschaffen, ohne hierfür das Entgelt von wenigen Euro entrichtet zu haben. Diesem Interesse standen jedoch überwiegende schutzwürdige Interessen der betroffenen Personen entgegen. Denn im Bereich des Drehkreuzes zum Solebecken legen betroffene Personen ihr Handtuch oder ihren Bademantel ab, um in das Becken zu gelangen. In den Zeiten des textilfreien Badens im Solebecken konnten sie somit gänzlich unbekleidet von der Kamera erfasst werden. Die Videoüberwachung in diesem Bereich haben wir aufgrund des unverhältnismäßigen Eingriffs in die Rechte und Freiheiten der betroffenen Personen untersagt. In diesem Bereich ging es nicht mehr um lebenswichtige Interessen und hochrangige Schutzgüter der Badegäste, sondern um die Wahrung rein wirtschaftlicher Interessen des Verantwortlichen. Die schutzwürdigen Interessen der betroffenen Personen waren an dieser Stelle schwerer zu gewichten. Wir haben diese Videoüberwachung daher per Anordnung untersagt. Die Anordnung wurde von der verantwortlichen Stelle auch akzeptiert, die Kamera wurde abgebaut.

06

KERNPUNKTE

Standard-Datenschutzmodell – neue Version, neue Bausteine

Software-Inventarisierung

Corona-Handreichungen zu Homeoffice und Videokonferenzen

6 Systemdatenschutz

Der Systemdatenschutz ist ein wichtiger Bestandteil in Verfahren und ihrer IT-Infrastruktur, um die Vorgaben der Artikel 25 und 32 DSGVO zum technisch-organisatorischen Datenschutz und zur Informationssicherheit umzusetzen. Im Berichtsjahr hat sich das ULD neben zahlreichen Einzelfällen und Grundsatzfragen (siehe auch Kapitel 10: „Aus dem IT-Labor“) primär mit den folgenden Bereichen beschäftigt: Zentrale Verfahren der Landesverwaltung (Tz. 6.1), deutschlandweite und internationale Zusammenarbeit der Datenschutzbeauftragten (Tz. 6.2) sowie Prüfungen und Beratungen (Tz. 6.3).

6.1 Landesebene

6.1.1 Zusammenarbeit mit dem Zentralen IT-Management (ZIT SH)

Das ULD wird regelmäßig als Gast zu den Sitzungen der IT-Beauftragten-Konferenz (ITBK) eingeladen. In dieser Konferenz, im Jahr 2020 überwiegend als Videokonferenz abgehalten, werden zentrale und ressortspezifische IT-Entwicklungen geplant und Entscheidungen von ressortübergreifender Bedeutung getroffen. Für das ULD ist die Teilnahme wichtig, um über zentrale IT-Entwicklungen informiert zu werden. Zusätzlich wurden dem ULD Planungen zu einzelnen IT-Vorhaben der Ressorts, die eine besondere Bedeutung oder eine große Reichweite haben, direkt durch das Zentrale IT-Management Schleswig-Holstein (ZIT SH) oder die Ressorts mitgeteilt.

Ein Schwerpunkt lag im Jahr 2020 in der Bereitstellung zusätzlicher IT-Ressourcen im Rahmen der Coronapandemie. Dies waren zum einen spezifische Fachanwendungen, insbesondere im Gesundheitsbereich, zum anderen der Ausbau und Bereitstellungen von Ressourcen für die mobile Büroarbeit: Der Ausbau betraf beispielsweise zusätzliche Kapazitäten für Telefonie, VPN-Einwahl und Netzkapazitäten. Zusätzliche Ressourcen waren ebenfalls für Videokonferenzdienste zur Nutzung von zentralen Videoräumen sowie vom Arbeitsplatz aus nötig.

Wie in den Vorjahren setzt sich die Tendenz zur **Zentralisierung von IT-Verfahren** weiter fort. Neben den bereits beschriebenen Herausforderungen bei der Umsetzung heterogener Anforderungen durch zentrale Systeme (38. TB, Tz. 6.1.1) gibt es Vorteile durch einheitliche Konfigurationsmöglichkeiten, mit denen sich beispielsweise Mindestsicherheitsanforderungen zentral vorgeben lassen. Ebenso lassen sich Neuentwicklungen, etwa bei der verstärkten **Nutzung von Open-Source-Software**, leichter für verschiedene Nutzergruppen verfügbar machen – etwa im Rahmen einer Softwarebereitstellung, die für die Büroarbeitsplätze der obersten Landesbehörden nur einmal erarbeitet und konfiguriert werden muss, dann aber bedarfsgerecht auf nahezu allen Rechnern installiert werden kann.

6.1.2 Sicherheitsmanagement der Landesverwaltung

Das Integrierte Sicherheitsmanagement des Landes wurde schon in vergangenen Tätigkeitsberichten dargestellt (z. B. 36. TB, Tz. 6.1). Nach einer Neuorganisation nimmt es nun wieder Fahrt auf. Neben den Informationssicherheitsbeauftragten der Ressorts und einzelner Teile der Landesverwaltung sind auch deren Datenschutzbeauftragte beteiligt. Der Landesrechnungshof und das ULD haben Gaststatus.

Nachdem die Leitlinie zur Informationssicherheit auf Landesebene neu gefasst und erlassen wurde, liegt derzeit der Fokus auf der Arbeit an **Richtlinien** und weiteren Detaildokumenten, die für die Arbeit vor Ort die Leitplanken vorgeben, gleichzeitig aber Raum für individuelle Besonderheiten lassen.

Auch das ULD beteiligt sich an der Mitarbeit an solchen Richtlinien, u. a. zur **Akten- und Datenträgervernichtung**: Es reicht beispielsweise nicht aus, per Telefonanruf Datenschutzpapiertonnen oder Aktenvernichtungsbehälter zu bestellen und darauf zu vertrauen, dass diese richtig – d. h. gemäß den jeweiligen Anforderungen des Datenschutzes – befüllt und entleert werden. Vielmehr gibt es je nach Sensibilität und Menge der Daten verschiedene Vernichtungsmöglichkeiten und Angebote der Dienstleister, die von einer besseren Altpapiertonne bis hin zu einer Vernichtung vor Ort unter Aufsicht des Verantwortlichen und ohne Einsichtsmöglichkeit des Dienstleisters reichen. Neben der Auswahl eines passenden Angebots sind vor Ort zahlreiche Details zu bedenken, etwa den Umgang mit Fehleinwürfen in solche Container (Wer darf diese öffnen, um den mutmaßlichen Fehleinwurf wieder herauszuholen?), den Standort in Gebäuden bis hin zur Abholung: Wer prüft beispielsweise, dass der „richtige“ Dienstleister die verschlossenen Container abholt und nicht jemand anders? Eine unbeaufsichtigte Bereitstellung auf dem Parkplatz, wie es bei Mülltonnen der Fall ist, erfüllt die Sicherheitsanforderungen selbstverständlich nicht.

Gegenstand der Richtlinie wird sein, alle wesentlichen Punkte anzusprechen, sodass für einen konkreten Einsatz entsprechende Entscheidungen getroffen werden. In anderen Detailfragen, bei denen es keine örtlichen Unterschiede gibt, können zentrale Festlegungen erfolgen.

Auch mit zunehmender Digitalisierung sind moderne **Multifunktionsgeräte** (Drucker, Kopierer, Scanner) mit ihren vielfältigen Funktionen und Diensten nicht mehr aus den Arbeitsabläufen wegzudenken. Dazu gehört z. B. das Kopieren von Dokumenten in unzähligen Varianten, das Drucken im Netz, das Scannen von Dokumenten mit Versand des gescannten Dokuments als E-Mail oder Fax. Häufig wird jedoch vergessen, dass es sich bei Multifunktionsgeräten um leistungsfähige Server handelt. Sie sind u. a. mit einem Prozessor, Arbeitsspeicher, Speichermedien, einer Netzkarte und einem Betriebssystem ausgerüstet und stellen Dienste für die angeschlossenen Clients (z. B. Arbeitsplatz-PC) zur Verfügung. Aus diesen Gründen sind sie sicherheitstechnisch als Server zu bewerten und müssen daher sorgfältig geplant, installiert, konfiguriert, implementiert, gewartet und dokumentiert werden. Neben den Aspekten der Datensicherheit muss zusätzlich gewährleistet sein, dass bei der Verarbeitung von Daten mit Multifunktionsgeräten die Betroffenenrechte nicht verletzt werden (37. TB, Tz. 10.4).

Daher wird für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten eine „**Rahmensicherheitsrichtlinie Kopierer, Scanner und Drucker**“ für Mindeststandards auf Grundlage des IT-Grundschutz-Kompendiums des BSI erstellt. Sie soll bei der Verarbeitung von Daten mit diesen Geräten sicherstellen, dass ein Sicherheitsniveau gewährleistet wird, das dem jeweiligen Schutzbedarf angemessen ist. Für die Berücksichtigung von Datenschutzaspekten in dieser Rahmensicherheitsrichtlinie ist das ULD in der Konzeptionsphase beteiligt.

6.1.3 Landesverordnungen zu Basisdiensten

Das Zentrale IT-Management des Landes (ZIT SH) stellt für die unmittelbare Landesverwaltung, aber auch für andere öffentliche Stellen des Landes und für Kommunen, IT-Verfahren als sogenannte Basisverfahren zur Verfügung.

Primär für die Landesverwaltung werden beispielsweise zentrale interne Verfahren wie E-Mail, Zeiterfassung und E-Akte bereitgestellt. Details hierzu werden in der **Zentrale-Stelle-Basisdienstever-ordnung (ZStBaDiVO)** geregelt. Einen ähnlichen Namen hat die **Basisdiensteverordnung (BasisdiensteVO)**. Regelungsgegenstand hier sind IT-Verfahren im Bereich des E-Governments, also solche Verfahren, bei denen Bürgerinnen und Bürger bzw. Unternehmen mit der Landes- oder Kommunalverwaltung in Kontakt treten. Dazu gehören u. a. zentral bereitgestellte Verfahren zur Umsetzung des Online-Zugangsgesetzes (OZG).

In beiden Fällen legt das ZIT SH wesentliche technische Details fest und verantwortet die Ordnungsmäßigkeit der Verfahren („Wie“). Für die mit diesen Verfahren verarbeiteten Inhalte („Was“) sind die einsetzenden Verwaltungen in datenschutzrechtlicher Hinsicht verantwortlich. Somit sind das ZIT SH einerseits als auch die einsetzenden Stellen andererseits gemeinsam verantwortlich. Diese gemeinsame Verantwortlichkeit ist schon seit

vielen Jahren gelebte Praxis, was sich u. a. in der Regelungsbefugnis des § 7 Abs. 4 LDSG ausdrückt.

Die Verantwortlichkeitstrennung, aber insbesondere die Schnittmengen und Überlappungen in einzelnen Teilbereichen sind regelungsbedürftig. Dies reicht von Festlegungen zu Test und Freigabe, zur Dokumentation, zu einer gegebenenfalls erforderlichen Datenschutz-Folgenabschätzung bis hin zur Vorgehensweise und zu gegenseitigen Informationspflichten bei Datenschutzverletzungen, damit u. a. eine Meldung an die Datenschutzaufsichtsbehörde und, wenn erforderlich, eine Benachrichtigung der betroffenen Personen erfolgt. Wesentliche Festlegungen werden im Wege der Verordnung getroffen; für Detailregelungen kommen Nutzungsvereinbarungen zum Einsatz.

Das ULD war beim (Neu-)Erlass der Verordnungen und auch bei einzelnen Nutzungsvereinbarungen beteiligt und konnte die **Regelungen im Hinblick auf Klarheit und Informationspflichten nachschärfen**. Dabei ist festzuhalten, dass zentrale Festlegungen zwar im Hinblick auf die örtlichen Gegebenheiten zu überprüfen, zu hinterfragen und gegebenenfalls anpassbar zu gestalten sind, aber zentrale Verfahren eben auch zentral gestaltet und verantwortet werden. So ist nicht jeder technische Anpassungswunsch erfüllbar; möglicherweise sind örtliche Prozessanpassungen notwendig.

Was ist zu tun?

Bei zentralen Verfahren, die für eine Vielzahl von beteiligten Stellen bereitgestellt werden, sind zahlreiche Fallkonstellationen und Besonderheiten zu beachten. Dies sollte von den zentralen Stellen bereits bei der Konzeption berücksichtigt werden, beispielsweise durch die Einbindung ausgewählter beteiligter Stellen. Sofern diese Besonderheiten nicht im Vorfeld erkannt und geregelt wurden, sind entsprechende Detailregelungen vorzunehmen.

6.2 Deutschlandweite und internationale Zusammenarbeit der Datenschutzbeauftragten

6.2.1 Arbeitskreis Technik

Auch im vergangenen Berichtszeitraum hat der Arbeitskreis Technik der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Reihe von Orientierungshilfen und Anwendungshinweisen erstellt, an deren Erarbeitung das ULD beteiligt war. In einigen Fällen waren dies eigenständige Unterlagen des AK Technik, in anderen Fällen technische Beiträge zu Dokumenten der Datenschutzkonferenz, z. B. zum Telemetrieverhalten des Betriebssystems Windows 10.

Herauszuheben ist die **„Orientierungshilfe Videokonferenzsysteme“**, die sich mit rechtlichen und technischen Fragestellungen von Videokonferenzsystemen (Tz. 6.3.2) befasst und für die konkrete Auswahl eines Systems eine Checkliste bereithält:

https://www.datenschutzzentrum.de/artikel/1343-Orientierungshilfe-Videokonferenzsysteme.html

Kurzlink: *https://uldsh.de/tb39-6-21a*

Ein weiterer Schwerpunkt war die Arbeit an einer **Orientierungshilfe zur E-Mail-Verschlüsselung**, die verschiedene Fallkonstellationen aufführt. Eine der Besonderheiten bei E-Mail-Verschlüsselung ist, dass Verschlüsselung sowohl bei der Sendung als auch beim Empfang (als Entschlüsselung) implementiert werden muss. Wie soll aber vorgegangen werden, wenn einer der Kommunikationspartner nicht „mitspielt“? Von Verantwortlichen wird zumindest erwartet, dass sie in der Lage sind, verschlüsselte E-Mails empfangen und senden zu können und bei bestimmten Inhalten die Verschlüsselung auch durchzusetzen, wenn sie das Medium E-Mail einsetzen wollen.

https://www.datenschutzkonferenz-online.de/media/oh/20200526_orientierungshilfe_e_mail_verschluesselung.pdf

Kurzlink: *https://uldsh.de/tb39-6-21b*

Ein weiterer Schwerpunkt waren das **Standard-Datenschutzmodell (SDM)** und Bausteine für die praktische Umsetzung von Datenschutzmaßnahmen (Tz. 6.2.2).

6.2.2 Das Standard-Datenschutzmodell – neue Version, neue Bausteine

Seit Ende 2019 haben sich deutschlandweit mit der Umsetzung von Datenschutzanforderungen befasste Institutionen zur Anwendung des Standard-Datenschutzmodells ausgesprochen. Die beharrliche Arbeit der letzten Jahre an einer **Standardisierung der Prüfmethode** zur Vermittlung von Recht und Technik und der Erstellung eines **Referenzkatalogs** mit Schutzmaßnahmen zahlt sich allmählich aus.

Das ULD hat das Standard-Datenschutzmodell (SDM) seit dem Entstehen 2012 maßgeblich geformt. 2016 hatte der Arbeitskreis Technik (AK Technik) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine **Unterarbeitsgruppe SDM** (UAGSDM) eingerichtet, die das ULD seitdem leitet.

Das SDM ist ein standardisiertes Prüf- und Beratungsverfahren (vgl. Art. 32 Abs. 1 Buchst. d DSGVO), mit der normative Anforderungen in funktionale Anforderungen überführt werden. Normative Anforderungen des Datenschutzrechts sind als Gebote und Verbote formuliert, während funktionale Anforderungen anhand ihrer Wirksamkeit oder Nichtwirksamkeit zu prüfen und zu beurteilen sind. Das SDM führt diese beiden Seiten, die rechtliche und die technische, systematisch und methodisch zusammen. Dabei hilft auf der technischen Seite der Ausweis von konkreten Standardschutzmaßnahmen zur Verminderung der Risiken für die Rechte und Freiheiten natürlicher Personen.

Drei Institutionen haben sich für die Umsetzung von Datenschutzanforderungen mithilfe des SDM ausgesprochen: Die DSK hat in ihrer 98. Konferenz am 19.11.2019 ohne Gegenstimme die Anwendung des SDM-V2b bei Prüfungen und Beratungen empfohlen. Der IT-Planungsrat – ein politisches Steuerungsgremium von Bund und Ländern (vgl. Art. 91c GG), das deren Zusammenarbeit im Bereich der Informationstechnik regelt – hat in dem Beschluss 2020/6 auf der 31. Sitzung am 25.03.2020 das SDM für die Planung, Anwendung und den Betrieb von personenbezogenen Verarbeitungen empfohlen. Ebenso verweist das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen der Modernisierung des Bausteins CON.2 „Datenschutz“ bei der Umsetzung von operativen Datenschutzanforderungen deutlich auf das SDM.

Katalog mit Bausteinen für Schutzmaßnahmen

Der AK Technik hat Anfang Oktober 2020 den folgenden Bausteinen zur Umsetzung von Schutzmaßnahmen gemäß DSGVO deutschlandweit zugestimmt:

- Aufbewahren
- Dokumentieren
- Protokollieren
- Trennen
- Löschen
- Berichtigen
- Einschränken

Das Handbuch zur Methode und die Texte zu den Bausteinen sind unter diesem Link abrufbar:

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Kurzlink: *https://uldsh.de/tb39-6-22a*

Aktuell wird an vorliegenden Entwürfen von Bausteinen gearbeitet, die auf der AK-Technik-Sitzung im Frühjahr 2021 verabschiedet werden sollen:

- Rollen zuteilen und berechtigen
- Planen und spezifizieren
- Anonymisieren
- Pseudonymisieren
- Sichern und wiederherstellen

Zu den folgenden Bausteinen sollen zur Frühjahrssitzung 2021 erste Entwürfe vorliegen:

- Daten minimieren
- Kryptokonzept
- Single Point of Contact
- Bereitstellen von Informationen

Die SDM-Methodik beschreibt in ihrer aktuellen Version den an einem permanenten Verbesserungsprozess orientierten Aufbau eines Datenschutzmanagementsystems (SDM-V2b, Seite 50 f.). Darüber hinaus sind Hinweise zur Umsetzung eines obligatorischen Einwilligungsmanagements (SDM-V2b, Seite 23) und zur Umsetzung aufsichtsbehördlicher Anweisungen (SDM-V2b, Seite 24) enthalten.

Das SDM enthält keine Hinweise zu den Projektphasen und der methodischen Durchführung einer Datenschutz-Folgenabschätzung (DSFA, vgl. Artikel 35 DSGVO), weil diese bereits vom Kurzpapier Nr. 5 aus dem Jahr 2018 abgedeckt sind. Das SDM hilft jedoch bei der methodischen Risikobearbeitung und der daraus folgenden Bestimmung der Maßnahmen für einen DSFA-Bericht.

Das Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO:

https://www.datenschutzzentrum.de/artikel/1162-.html

Kurzlink: *https://uldsh.de/tb39-6-22b*

Geltung von „Muss-Anforderungen“

Zu den in den SDM-Bausteinen aufgeführten Maßnahmen wird häufig die Frage gestellt, welche Geltung die Anforderungen des SDM auf der Ebene der Referenzmaßnahmen zur Umsetzung der Anforderungen der DSGVO beanspruchen. Muss ein Verantwortlicher unmittelbar eine Sanktion erwarten, wenn er nicht eine Maßnahme aus dem SDM-Katalog umsetzt?

Das SDM lehnt sich methodisch an den IT-Grundschutz des BSI an. Dort findet sich eine Sprachregelung zum Grad der Verpflichtung, mit dem eine Maßnahme umzusetzen ist, nämlich die Unterscheidung von MUSS (oder ähnlich: Formulierungen wie „darf nur“, „darf nicht“) und SOLLTE (ebenso: „sollte nicht“). Dieser Sprachregelung folgt das SDM. Ein MUSS bedeutet, dass „so gekennzeichnete Anforderungen unbedingt erfüllt werden müssen“. Ein SOLLTE bedeutet, „dass eine Anforderung zwar normalerweise erfüllt werden muss, bei stichhaltigen Gründen aber auch davon abgesehen werden kann“.

Beim IT-Grundschutz des BSI ist die Geltung einer „Muss-Maßnahme“ – abgesehen vom Kontext kritischer Infrastrukturen und dem BSI-Gesetz – nicht mit gesetzlichen Vorgaben begründet. Jedoch leiten sich solche Umsetzungsverpflichtungen des IT-Grundschutzes aus dem Bekenntnis der Geschäftsleitung zur Informationssicherheit und materiell aus dem Stand der Technik ab, wovon auch „Good Practice“ in Bezug auf Regeln und Prozesse umfasst wird. In einigen Fällen verweisen IT-Sicherheitsbeauftragte zusätzlich auf Artikel 32 der DSGVO. Allerdings werden diese Maßnahmen typischerweise zur Sicherung der Geschäftsprozesse genutzt und haben die Durchsetzung der Rechte der Betroffenen – wie in der DSGVO gefordert – nicht im Fokus.

Die Geltung der Maßnahmen des operativen Datenschutzes leitet sich dagegen unmittelbar aus den Datenschutzgesetzen (Spezialgesetzen, DSGVO, BDSG, LDSG) sowie den bilateralen Einwilligungen und Verträgen ab. Materiell ist dabei ebenfalls der Stand der Technik (nicht der Stand von Wissenschaft und Forschung) der verpflichtende geltende Maßstab zur Umsetzung angemessen wirkungsvoller Maßnahmen (Artikel 25 und Artikel 32 DSGVO).

Im SDM wird ganz überwiegend die Formulierung „SOLLTE“ gewählt, wenn es um die konkrete Ausgestaltung spezifischer Schutzmaßnahmen geht. Das heißt also, dass in begründeten Fällen von einer Standardmaßnahme, wie sie das SDM in seinem Katalog generischer Maßnahmen ausweist, abgewichen werden darf. Wesentlich ist aber, dass die Datenschutzanforderung – ob über den Weg einer Standardmaßnahme oder auf andere Weise – erreicht wird. Das SDM will auch in diesen Fällen dabei helfen, dass „die funktionale Äquivalenz der Wirksamkeit“ auch der Alternativmaßnahmen nachgewiesen werden kann (SDM-V2b, Seite 58).

Was ist zu tun?

Um ihre Rechenschaftspflicht zu erfüllen, müssen Verantwortliche Sorge dafür tragen, dass die Datenschutzanforderungen umgesetzt werden. Dabei ist der Einsatz eines standardisierten, methodisch-systematischen Verfahrens zur Prüfung und operativen Umsetzung der DSGVO angeraten.

6.3 Ausgewählte Ergebnisse aus Beratungen und Prüfungen

6.3.1 Zusammenarbeit mit den Spitzenorganisationen der Gewerkschaften: Software-Inventarisierung, Internet- und E-Mail-Nutzung

Die Einbindung des ULD in die Zusammenarbeit der Landesbehörden, insbesondere des ZIT SH, mit den Spitzenorganisationen der Gewerkschaften setzte sich auch im Berichtszeitraum fort.

Zu den Schwerpunkten im Jahr 2020 gehörte eine geplante Regelung zur **Software-Inventarisierung auf Arbeitsplatzrechnern**. Hintergrund ist die Tendenz von Softwareanbietern, eine verlässliche Auskunft über die Anzahl der tatsächlich installierten Software-Instanzen einzufordern und mit der Anzahl der beschafften Lizenzen zu vergleichen, um eventuelle Unterlizensierungen feststellen zu können – diese Anforderung ist häufig Bestandteil von Software-Rahmenverträgen. Eng damit zusammenhängend ist die effektive Nutzung vorhandener Softwarelizenzen auf Arbeitsplatzrechnern, indem zentral nicht mehr benötigte Software erkannt, deinstalliert und dann auf den Arbeitsplatzrechnern bereitgestellt wird, auf denen sie erforderlich ist.

Für beide Fälle ist es erforderlich, die auf Arbeitsplatzrechnern installierte Software zu inventarisieren und in einer Übersicht zusammenfassen zu können. Zwar gibt es Werkzeuge zum Inventarisieren und Verwalten von Software, doch haben diese meist einen anderen Fokus: etwa technische Übersichten zur Konfiguration eines Geräts, haushalterische Inventarisierungen oder Mechanismen, um erforderliche Sicherheitsupdates bereitstellen zu können.

Datenschutzrechtlich spannend wird es, wenn neben dem Vorhandensein von Software auf dienstlichen Rechnern auch deren Nutzung nachvollzogen wird, etwa in der Form **„letzte Nutzung am XXX um YYY“**. Da Arbeitsplatzrechner heutzutage meist individuell einzelnen Personen zugeordnet sind, wären Rückschlüsse auf das individuelle Arbeitsverhalten möglich. Dies ist nicht Zweck der Inventarisierung.

Hier ist geplant, den **Detaillierungsgrad der Einsichtsrechte zu staffeln**: Für einige Beteiligte ist nur die Anzahl der installierten Lizenzen relevant, für andere ist es wesentlich, um welche Rechner es sich handelt, auf denen die Software tatsächlich installiert ist und dort gegebenenfalls deinstalliert wird. Das ULD begleitet die Erstellung einer Regelung.

Ein weiterer Schwerpunkt war wie im Vorjahr (38. TB, Tz. 6.3.1) die Überarbeitung der **59er-Vereinbarung zur privaten Nutzung von Internet und E-Mail am Arbeitsplatz**, da sich hier die Protokollierungsdauer für Internetzugriffe deutlich verlängern soll.

59er-Vereinbarung

Vereinbarungen gemäß § 59 Mitbestimmungsgesetz zwischen den Spitzenorganisationen der Gewerkschaften und der zuständigen obersten Landesbehörde, die als allgemeine Mitbestimmungsregelungen über den Geschäftsbereich einer obersten Landesbehörde hinausgehen („Dienstvereinbarung auf Landesebene“).

Protokolliert werden **Daten zur Verbindung** (welches Gerät hat wann zu welchem Server eine Verbindung; Inhaltsdaten sind nicht Gegenstand der Protokolle). Dabei ist zwischen verschiedenen Gründen einer Protokollierung zu unterscheiden:

- Gründe der Arbeitsorganisation (z. B. zur Feststellung von Art und Umfang der Nutzung und zur Missbrauchskontrolle),
- Gründe der Systemtechnik (z. B. zur Fehlerverfolgung),
- Gründe der Daten- und Systemsicherheit.

Aus Sicht der Arbeitsorganisation geht es um **Internetzugriffe durch Beschäftigte**, die sich hinsichtlich Art und Umfang **außerhalb des festgelegten Rahmens** bewegen. Hierzu gibt es schon seit vielen Jahren ein erprobtes Vorgehen mit einer **gestuften Protokollauswertung**, die zunächst aggregierte Daten betrachtet. Sollten Warnungen fruchtlos bleiben, ist bei fortgesetzten Verstößen eine Protokollierung bis hin zu einzelnen Personen möglich. Diese Mechanismen und zeitlichen Beschränkungen der Zugriffsmöglichkeiten sollen nicht verändert werden.

Bei der **Protokollierung aus sicherheitstechnischer Sicht** geht es in erster Linie um Internetzugriffe, die von einem Gerät aus erfolgen, um **Schadcode** aus dem Internet herunterzuladen. Dies kann versehentlich durch einen Nutzer beim Browsing erfolgen, aber auch ohne Nutzerinteraktion durch eine Schadsoftware geschehen, die zeitverzögert und eigenständig weitere Bestandteile aus dem Internet nachlädt (Stichwort: Emotet). Um diese Rechner im Netz identifizieren und von Schadcode bereinigen zu können, ist eine **längerfristige Protokollierung der Internetzugriffe auf Geräteebene** erforderlich: Von bestimmten Internetadressen wird erst mit einer zeitlichen Verzögerung bekannt, dass sie zur Bereitstellung von Schadcode genutzt wurden.

In beiden Fällen werden die Verbindungen der Geräte protokolliert. Die Zuordnung zu handelnden Personen bzw. zu den Personen und Nutzerkonten, die die Geräte benutzt haben, erfolgt in einem zweiten Schritt. Dies erlaubt es, die Zugriffsmöglichkeiten auf die Protokolle eng zu begrenzen und eine Zuordnung zu Personen nur im Bedarfsfall vorzunehmen – etwa in dem gestuften Verfahren zur Missbrauchskontrolle oder wenn tatsächlich das Risiko besteht, dass Rechner oder Nutzerkonten infiziert sind.

Aus Datenschutzsicht ist eine längerfristige Protokollierung von überwiegend „harmlosen“ Zugriffen der Beschäftigten kritisch zu betrachten. Besser wäre eine effiziente Blockade aller Zugriffe auf Schadsoftware, die allerdings derzeit nicht realistisch ist (u. a. deshalb, weil sich bestimmte Zugriffe erst Tage oder Monate später als schadensstiftend herausstellen). Auf der anderen Seite ist die Integrität der Hard- und Software der Landesverwaltung ein hohes Gut, denn bei einem Befall mit Schadcode sind personenbezogene Daten von Bürgerinnen und Bürgern unmittelbar betroffen – solche Fälle kennen wir von zahlreichen Meldungen zu Datenschutzvorfällen gemäß Artikel 33 DSGVO über Verschlüsselungstrojaner und Co. Dies ist bei der Abwägung zum Detaillierungsgrad der Protokollierung und zur Dauer der Speicherung einzubeziehen.

6.3.2 Dauerbrenner Videokonferenzen

Ein Dauerthema war im vergangenen Berichtszeitraum das Thema Videokonferenzen. Insbesondere gab es zahlreiche Anfragen zu einzelnen Anbietern, zu technischen Details sowie Bitten um Produktempfehlungen für spezifische Anwendungsfälle.

Vor der Auswahl eines Produkts ist es sinnvoll, zunächst die **Anwendungsfälle genauer zu betrachten**. Bei der Analyse hilft oft ein Vergleich mit einer realen Konferenz: Handelt es sich um eine hochvertrauliche Besprechung von wenigen Personen (vergleichbar einem ärztlichen Gespräch), um eine Besprechung mit begrenztem Nutzerkreis (etwa ein Bewerbungsgespräch, eine Arbeitsgruppenbesprechung oder ein Klassenraumszenario), einen Vortrag (d. h. im Wesentlichen nur eine Rednerin oder ein Redner) oder eine Veranstaltung, die auch an die Öffentlichkeit übertragen werden soll (etwa eine öffentliche Sitzung, Tz. 4.1.3)?

So wie auch in der analogen Welt für diese Anwendungsfälle verschiedene Räume (z. B. Büro, Sitzungszimmer, Vortragssaal) und verschiedene Arten der Eingangskontrolle (z. B. mit Anmeldung, öffentlich zugänglich) genutzt werden, eignen sich die verschiedenen angebotenen Videokonferenzsysteme in unterschiedlichem Maße. Die Analogie setzt sich fort in der Frage, ob eigene oder fremde Räumlichkeiten verwendet werden sollen – bei Videokonferenzsystemen ist es die Frage, ob ein selbst betriebenes System zum Einsatz kommt oder ob auf einen der zahlreichen Anbieter, die solche Dienste auf dem Markt bereitstellen, zurückgegriffen werden soll.

Es gibt relativ einfache selbst betriebene Konferenzsysteme, bei dem Menschen wie bei einem spontanen Treffen in einer Kaffeeküche oder unter Nachbarn auf der Straße zusammenkommen und dann miteinander interagieren. Es gibt komplexere selbst betreibbare Systeme, die beispielsweise einen virtuellen Vorraum bieten, bei denen neue Teilnehmende virtuell anklopfen müssen, bevor eine Leitung oder Moderation die neuen Teilnehmenden in die Konferenz hineinnimmt und dann obendrein die Sendung der Videobilder und Audiodaten steuern kann. Solche Konferenzsysteme kommen zunehmend in Bildungsplattformen zum Einsatz. Weitere Beispiele sind Messengerdienste,

die Echtzeitübertragung von Audio- und Videodaten ermöglichen – zumindest in einem Zwei-Personen-Gespräch.

Eine zusätzliche Parallele lässt sich bei der Frage der Zugänglichkeit und Sicherheit ziehen: Können alle Teilnehmenden den realen Sitzungsraum einfach erreichen und drohen beim Aufenthalt keine Risiken, etwa durch Baumängel? In der Welt der Videokonferenzen lauten diese Fragen sinngemäß, ob spezielle technische Voraussetzungen wie Hard- und Software (etwa Apps) erforderlich sind und ob die Informationssicherheit, etwa durch schadhafte Software, gefährdet ist.

Es gibt aber auch Grenzen der Analogie: Anders als bei der Anmietung von Räumlichkeiten für eine Veranstaltung stellen sich bei Videokonferenzsystemen unmittelbar Fragen der datenschutzrechtlichen Verantwortlichkeit, denn es werden **Video- und Audiodaten von Teilnehmenden** verarbeitet, teilweise die Sitzungen auch eigens gespeichert. Hinzu kommen in jedem Fall **technische Metadaten** darüber, welche Person wann von welchem IT-System an welcher Konferenz teilgenommen hat. Darüber hinaus kann es sich bei den Inhaltsdaten um vertraulich zu haltende Informationen wie **personenbezogene Daten Dritter** handeln, wenn beispielsweise in einer Konferenz über Personen gesprochen wird.

Dies führt relativ schnell zu der Frage, inwieweit der technische Betreiber eines Videokonferenzsystems Kenntnis von den Inhalten nehmen kann. Zumindest bei Zwei-Personen-Gesprächen bieten die meisten Systeme eine **Ende-zu-Ende-Verschlüsselung der Gesprächsinhalte** an; mittlerweile gibt es auch Systeme, die bei Mehr-Personen-Konferenzen die Daten so verschlüsseln, dass der technische Betreiber keine Einsicht in die Daten bekommt. Somit sollten Verantwortliche ein System bzw. einen Anbieter wählen, das bzw. der diese Funktionalität bereitstellt. Allerdings sind bei einer effektiven Ende-zu-Ende-Verschlüsselung einer Videokonferenz bestimmte Funktionen wie Telefoneinwahl oder zentrale Aufzeichnung (derzeit) nicht möglich.

Während eine eigenständig betriebene Konferenzplattform aus datenschutzrechtlicher Sicht vergleichsweise einfach ist, stellen sich bei der Nutzung von Systemen Dritter zahlreiche Fragen – bis hin zu der Frage, welche Datenverarbeitung in Bezug auf (Meta-)Daten der Teilnehmenden erfolgt und inwieweit der Systemanbieter dafür allein oder gemeinsam verantwortlich ist. Teilweise berufen sich außereuropäische Anbieter auf (mittlerweile ungültige) Rechtsgrundlagen wie Privacy Shield.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat Anforderungen an Videokonferenzsysteme in einer Orientierungshilfe sowie einer Checkliste zusammengestellt:

https://www.datenschutzzentrum.de/artikel/1343-Orientierungshilfe-Videokonferenzsysteme.html

Kurzlink: *https://uldsh.de/tb39-6-32*

Was ist zu tun?

Die zu Beginn der Coronakrise oft recht hemdsärmelig eingeführten Verfahren für Videokonferenzen müssen auf ein solides rechtliches und technisches Fundament gestellt werden.

6.3.3 Corona-Handreichungen zu Homeoffice und Videokonferenzen

Plötzlich … arbeitet man im **Homeoffice** oder nimmt an **Videokonferenzen** teil. Die Coronapandemie hat den Arbeitsalltag und die Arbeitsabläufe von einem Tag auf den anderen verändert, und viele Beschäftigte fanden sich unvermittelt im Homeoffice wieder.

Auch für viele Behörden und Unternehmen wie auch für ihre Mitarbeiterinnen und Mitarbeiter war das neu. Sie mussten innerhalb kurzer Zeit die Heimarbeitsplätze mit der entsprechenden Technik ausrüsten und auch die Arbeitsabläufe und die Kommunikation mit den Kolleginnen und Kollegin-

nen untereinander organisieren. Das bedeutete in vielen Fällen **Improvisation**. Damit die Arbeit im Homeoffice nicht zu einem **Datenschutzrisiko** wird, hat das ULD zwei Handreichungen veröffentlicht. Beide geben einen Überblick darüber, wie man mithilfe von einfachen Maßnahmen in der Übergangszeit – zwischen der improvisierten Aufrechterhaltung des Arbeitsalltags bis hin zu einem technisch und organisatorisch geregelten Arbeitsablauf – personenbezogene Daten gegen eine unberechtigte Kenntnisnahme schützen kann.

Die Veröffentlichung „Datenschutz: Plötzlich im Homeoffice – und nun?“ beschreibt einfache Regeln und Hinweise für den Umgang mit personenbezogenen Daten, die alle Mitarbeitenden an ihren Homeoffice-Arbeitsplätzen umsetzen können. Dabei werden verschiedene praktische und organisatorische Szenarien betrachtet, wie

- der Transport von Dokumenten und IT-Geräten vom Arbeitsplatz ins Homeoffice,
- die Einrichtung des Arbeitsplatzes im Homeoffice,
- organisatorische Fragestellungen, die in der Kommunikation mit Vorgesetzten und im Kollegium geklärt werden müssen, und
- Sicherheitsmaßnahmen, die am Arbeitsplatz im Homeoffice umgesetzt werden können, auch wenn es noch keine allgemeinen Maßnahmen in Form von Betriebs- bzw. Dienstanweisungen gibt.

Die Veröffentlichung „Datenschutz: Plötzlich Videokonferenzen – und nun?“ beschäftigt sich im Gegensatz zu anderen Veröffentlichungen (siehe auch Tz. 6.3.2) nicht mit den Vor- bzw. Nachteilen einzelner Videokonferenzsysteme, sondern legt den Schwerpunkt auf einfache Regeln und Hinweise für den Umgang mit personenbezogenen Daten beim Einsatz von Videokonferenzen.

Mit der Übertragung von Bildern und Tönen von Personen werden automatisch personenbezogene Daten übertragen, je nach Inhalt der Konferenz können noch sensiblere oder weitere Daten von Dritten hinzukommen. Personen, die eine Videokonferenz organisieren, und Personen, die an einer Videokonferenz teilnehmen, können unterschiedliche Maßnahmen zum Schutz personenbezogener Daten treffen. Aus diesem Grund werden sie in dieser Handreichung differenziert betrachtet.

Nach einer **grundsätzlichen Betrachtung**, ob eine Videokonferenz für einen bestimmten Zweck das richtige Kommunikationsmittel darstellt, und einer Identifizierung, welche personenbezogenen Daten während der Videokonferenz betroffen sein können, orientiert sich die Handreichung an einem typischen Ablauf einer Videokonferenz:

- Schon bei der **Vorbereitung** können viele datenschutzrechtliche Probleme vermieden werden, z. B. bei der Auswahl der Technik oder der Gestaltung des Umfelds.
- Sowohl vor als auch während der Videokonferenz sollten die **angebotenen Funktionen** daraufhin überprüft werden, ob eine datenschutzfreundliche Voreinstellung möglich ist, z. B. Aufnahmefunktion, Integration von sozialen Medien usw.
- Auch mit dem **eigenen Verhalten** während einer Videokonferenz kann vermieden werden, dass sensible Informationen weitergegeben werden, z. B. durch das Ausschalten der Kamera, wenn unbeteiligte Personen in das Sichtfeld der Kamera kommen.

Schon der Name dieser Corona-Veröffentlichungen **„Plötzlich … – und nun?“ gibt einen Hinweis auf die zeitliche Eingrenzung dieser Hinweise**. Sie dienen lediglich zur **Überbrückung**

- einer improvisierten Lösung,
- einer konzeptionellen Phase, in der eine der Datenverarbeitung angemessene Erforderlichkeits- und Risikobetrachtung durchgeführt wird sowie technische und organisatorische Maßnahmen zu Datenschutz und Datensicherheit festgelegt werden,
- bis hin zu dokumentierten Betriebs- bzw. Dienstanweisungen, die die Mitarbeitenden über die zu treffenden Verhaltensregeln informieren.

Die Veröffentlichungen können auf der Webseite des ULD heruntergeladen werden:

https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf

Kurzlink: *https://uldsh.de/tb39-6-33a*

https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-videokonferenzen.pdf

Kurzlink: *https://uldsh.de/tb39-6-33b*

07

KERNPUNKTE

Coronamaßnahme WLAN-Tracking für „Strandampel“

Facebook-Fanpages

Gemeinsame Prüfung von Online-Medien

7 Neue Medien

Ein Querschnittsthema des Datenschutzes betrifft die sogenannten Neuen Medien. Auch wenn sich die Fälle nicht trennscharf von anderen Beschwerden oder Prüfungen abgrenzen lassen, in denen es vielfach auch um Themen der Digitalisierung geht, heben wir einige Punkte in diesem Kapitel heraus, weil besondere Konstellationen vorliegen und teilweise neben der Datenschutz-Grundverordnung auch die ePrivacy-Richtlinie eine Rolle spielt, deren Reform weiter auf sich warten lässt. Im Folgenden berichten wir von der Nutzung von WLAN-Tracking zur Bestimmung der Personendichte als Coronamaßnahme (Tz. 7.1), von Verfahren zu Facebook-Fanpages (Tz. 7.2) und von einer gemeinsamen Prüfung der Datenschutzaufsichtsbehörden im Bereich der Online-Medien (Tz. 7.3).

7.1 Coronamaßnahme WLAN-Tracking zur Bestimmung der Personendichte

Im Zusammenhang mit der Bekämpfung der Coronapandemie haben vereinzelte Ordnungsbehörden in Schleswig-Holstein die dem WLAN-Tracking zugrunde liegende Technik genutzt, um die Personendichte in Freizeiteinrichtungen zu messen und potenzielle Besucher über ein im Internet abrufbares Ampelsystem auf den Grad des **Risikos einer zu großen Personendichte** hinzuweisen, z. B. am Strand („Strandampel“).

WLAN-Tracking

Erhebung von Daten, die mobile Endgeräte, wie z. B. Smartphones, bei entsprechender Konfiguration aussenden (MAC-Adressen). Die Aussendung von MAC-Adressen durch Endgeräte findet eigentlich statt, um eine schnelle und einfache Verbindung der Endgeräte mit offenen Netzzugangspunkten (z. B. WLAN-Hotspots) zu ermöglichen. Werden diese Daten jedoch von dazu geeigneten Empfangsgeräten, die sich wie ein WLAN-Hotspot darstellen, erhoben und verarbeitet, können die Daten beispielsweise dazu verwendet werden festzustellen, ob und wie viele verschiedene Endgeräte sich an einem Ort aufhalten. Je nachdem welche weitere Verarbeitung stattfindet, lassen sich aus den erhobenen Daten noch weitere Informationen ziehen. Ein typisches Anwendungsfeld ist die Messung von Besucher- oder Kundenströmen.

Beim WLAN-Tracking werden MAC-Adressen der Endgeräte erfasst. **Bei MAC-Adressen (auch virtuellen, dynamischen) handelt es sich um personenbezogene Daten nach Art. 4 Nr. 1 DSGVO.** Eine Zuordnung ist möglich, auch wenn dies nur mittels eines gewissen technischen Aufwands der Fall ist.

Dieser Fall unterscheidet sich von anderen (siehe auch die Fälle zu Offline-Tracking und Ortung von Mobiltelefonen in einer Fußgängerzone, 37. TB, Tz. 5.4.8) insbesondere durch seinen Zweck: die Coronamaßnahme, eine zu große Personendichte zu erkennen und darauf aufbauend weiter gehende Maßnahmen im Sinne des Infektionsschutzes zu ergreifen, beispielsweise den Zugang zu den Orten einzuschränken. Bezüglich der Zulässigkeit einer solchen Datenverarbeitung und des Risikos für die Rechte und Freiheiten betroffener Personen ist die konkrete Ausgestaltung der Verarbeitung zu berücksichtigen:

Um den vor Ort betroffenen Personen zu ermöglichen, die WLAN-Signalaussendung in den mitgeführten Endgeräten abzuschalten und somit eine Erhebung personenbezogener Daten zu verhindern, können Schilder angebracht werden, die auf den Umstand der Erhebung hinweisen. Eine solche Maßnahme fand sich in einem früheren Entwurf einer Verordnung über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, die die noch gültige entsprechende Richtlinie (ePrivacy-Richtlinie) ablösen soll. Der Verordnungsentwurf sah vor, das Thema WLAN-Tracking gesetzlich zu regeln. Eine Warnbeschilderung war dabei eine von mehreren vorgeschlagenen Maßnahmen.

Weiterhin sind die Pflichtinformationen nach Art. 13 Abs. 1 und 2 DSGVO zu erfüllen. Dies kann etwa durch Aushänge erfolgen.

Eine Verkettungsmöglichkeit der personenbezogenen Daten, die Bewegungsprofile ermöglichen würde, kann dadurch ausgeschlossen werden, dass nicht die erhobenen MAC-Adressen gespeichert werden, sondern diese nach einer Erhebung und Erfassung gelöscht werden und stattdessen eine fortlaufende Nummer im System verwendet wird. Begibt sich eine betroffene Person mit ihrem Endgerät erneut in den Empfangsbereich, wird erneut die dann ausgesendete (gegebenenfalls virtuelle, dynamische) MAC-Adresse erfasst und wieder eine fortlaufende Nummer vergeben. Es wird nicht die Angabe erfasst, dass es sich um dasselbe Smartphone handelt, da ein Abgleich mangels Speicherung nicht möglich wäre. Die fortlaufenden Nummern dienen der Zählung, wie viele Personen den Erfassungsbereich durchschreiten, um pandemiebedingt gegebenenfalls ordnungsbehördlich auf eine zu hohe Besucheranzahl reagieren zu können.

Die Erhebung und weitere Verarbeitung von MAC-Adressen kann in diesem Fall unter bestimmten engen Voraussetzungen zur pandemiebedingten Erfassung durch eine öffentliche Stelle als datenschutzrechtlich Verantwortliche auf die Rechtsgrundlage des Art. 6 Abs. 1 Buchst. e DSGVO in Verbindung mit § 3 Abs. 1 LDSG gestützt werden. Danach ist die Verarbeitung zulässig, soweit diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Dabei kann es sich um die Wahrnehmung von ordnungsbehördlichen Aufgaben der Gefahrenabwehr handeln. Die Arbeit der Ordnungsbehörden kann gefördert werden, indem Brennpunkte für eine hohe Besucherdichte auf öffentlichen Plätzen (Eingangsbereiche zu öffentlichen Einrichtungen, Marktplätze) identifiziert werden, um dann Abstandsregeln und andere Verpflichtungen durchsetzen zu können. Die Rechtsgrundlage für eine kurzzeitige Erhebung der MAC-Adressen ist daher im Gefahrenabwehrrecht der Ordnungsbehörden zu suchen.

Ausgehend davon, dass die Befugnis zur Kontrolle der Abstandsregeln durch die datenschutzrechtlich verantwortliche Gemeinde besteht, ist die Bekämpfung der Coronapandemie ein zulässiger Zweck bzw. eine Aufgabe im öffentlichen Interesse nach Art. 6 Abs. 1 Buchst. e DSGVO.

Sichergestellt sein muss, dass eine Verarbeitung personenbezogener Daten zu anderen, damit inkompatiblen Zwecken nicht erfolgt. Eine solche wäre – mangels Rechtsgrundlage – unzulässig.

Mit dem etwaigen künftigen Wegfall einer ordnungsbehördlichen Kontrollbedürftigkeit (nach der Coronapandemie) darf das System der Erfassung von MAC-Adressen **nicht mehr genutzt** werden, da der zulässige Verarbeitungszweck dieses spezifischen Falls dann nicht mehr besteht.

7.2 Verfahren zu den Facebook-Fanpages

Auf Vorlage des Bundesverwaltungsgerichts hat der Gerichtshof der Europäischen Union (EuGH) mit Urteil vom 05.06.2018 (Rs. C-210/16 „Wirtschaftsakademie“) entschieden, dass der Betreiber einer Fanpage für die durch Facebook erfolgende Datenverarbeitung mitverantwortlich ist. Denn er ermöglicht durch den Betrieb der Fanpage Facebook den Zugriff auf die Daten der Fanpage-Besucherinnen und -Besucher.

Das Bundesverwaltungsgericht hat auf der Grundlage dieser bindenden Vorgabe mit Urteil vom 11.09.2019 das Berufungsurteil aufgehoben und den **Rechtsstreit an das Schleswig-Holsteinische Oberverwaltungsgericht (OVG Schleswig) zurückverwiesen**. Die Beurteilung der Rechtswidrigkeit der Datenverarbeitung im Zusammenhang mit dem Betrieb der Facebook-Fanpage muss nun nach den gesetzlichen Regelungen (insbesondere nach dem Telemediengesetz) erfolgen, die zum Zeitpunkt der letzten Behördenentscheidung im Jahr 2011 galten. Im Verfahren vor dem OVG Schleswig haben die Beteiligten sich bisher lediglich schriftlich geäußert. Ein Verhandlungstermin wurde noch nicht bekannt gegeben.

Auf Grundlage u. a. des EuGH-Urteils „Wirtschaftsakademie“ hat der Europäische Datenschutzausschuss (EDSA) „Guidelines on the targeting on social media users“ verabschiedet (siehe auch Tz. 11.2) und darin ausgeführt, welchen Verpflichtungen gemeinsam Verantwortliche unterliegen. Bezüglich der Verpflichtung, eine Vereinbarung nach Artikel 26 DSGVO zu treffen, und zu der Frage der Rechtsgrundlage heißt es dort:

„If, for example, the controller is considering to rely on Article 6(1)(f) GDPR as a legal basis, it is necessary, among other things, **to know the extent of the data processing** in order to be able to assess whether the interest of the controller(s) are overridden by the interests or fundamental rights and freedoms of the data subjects. Without sufficient information concerning the processing, such an assessment cannot be performed. The importance of **including or referencing the necessary information in the context of a joint arrangement** cannot be overstated, especially in situations where one of the parties almost exclusive has the knowledge and access to the information necessary for both parties to comply with the GDPR.“ (Guidelines 08/2020 on the targeting of social media users, Seite 33 f.)

Auf den Fall der Facebook-Fanpages bezogen, bedeutet dies, dass die **Fanpage-Betreiber ausreichende Informationen erhalten müssen, um die Interessen und Rechte und Freiheiten der betroffenen Personen abschätzen zu können**.

Diese Informationen über die Datenverarbeitung durch Facebook gehören demnach in die Vereinbarung nach Artikel 26-DSGVO, die jeder Fanpage-Betreiber mit Facebook schließen muss.

Die Leitlinien sind unter dem folgenden Link abrufbar:

https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_de

Kurzlink: *https://uldsh.de/tb39-7-2*

7.3 Gemeinsame Prüfung der Gestaltung der Webseiten von Online-Medien

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in der Vergangenheit wiederholt kritisch darauf hingewiesen, dass der Gesetzgeber Art. 5 Abs. 3 ePrivacy-Richtlinie (2002/58/EG, zuletzt geändert durch die Richtlinie 2009/136/EG, auch als „Cookie-Richtlinie“ bezeichnet) nicht oder nicht ordnungsgemäß umgesetzt hat. Nach Art. 5 Abs. 3 der Richtlinie haben die Mitgliedstaaten sicherzustellen, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen seine Einwilligung gegeben hat. Ausnahmen von diesem grundsätzlichen Einwilligungserfordernis greifen nur dann, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Das deutsche Recht bildet die klaren Vorgaben der ePrivacy-Richtlinie im Telemediengesetz bis heute nicht ab. Stattdessen findet sich in § 15 Abs. 3 TMG die Vorgabe, dass für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellt werden dürfen, sofern die Nutzerinnen und Nutzer dem nicht widersprechen.

Die DSK hat bereits im April 2018 in der Positionsbestimmung „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“ den Standpunkt vertreten, dass die Datenschutzvorschriften des Telemediengesetzes neben der Datenschutz-Grundverordnung (DSGVO) nicht mehr anwendbar sind. Eine ausführliche Begründung zu dieser Rechtsauffassung wurde von der DSK in der Orientierungshilfe für Anbieter von Telemedien im März 2019 veröffentlicht (Positionsbestimmung der DSK vom 26. April 2018 „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“).

Die Orientierungshilfe ist unter dem folgenden Link abrufbar:

https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

Kurzlink: *https://uldsh.de/tb39-7-3*

Mit Urteil vom 01.10.2019 hat der Europäische Gerichtshof (EuGH) auf Vorlage des Bundesgerichtshofs (BGH) entschieden, dass keine wirksame Einwilligung im Sinne der ePrivacy-Richtlinie und der DSGVO vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät der Nutzerin oder des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das die Nutzerin oder der Nutzer zur Verweigerung seiner Einwilligung abwählen muss (EuGH, Urteil vom 01.10.2019, Rs. C-673/17 „Planet49“).

Ausgehend von diesem Urteil hat der BGH mit Urteil vom 28.05.2020 die Vorschrift des § 15 Abs. 3 TMG mit dem Ziel einer europarechtskonformen Umsetzung von Art. 5 Abs. 3 ePrivacy-Richtlinie ausgelegt und angenommen, dass in dem Fehlen einer wirksamen Einwilligung ein solcher Widerspruch gesehen werden könne, weshalb in solchen Fällen, die § 15 Abs. 3 TMG regelt, eine aktive Einwilligung erforderlich sei (BGH, Urteil vom 28.05.2020 – I ZR 7/16).

Nach der Veröffentlichung der Orientierungshilfe der DSK sowie nach der Verkündung der Urteile von EuGH und BGH erreichte uns eine Vielzahl von Kontrollanregungen und Beschwerden in Bezug auf die Gestaltung von Webseiten schleswig-holsteinischer Verantwortlicher, bei denen in den allermeisten Fällen die Vorgaben nicht oder nicht hinreichend eingehalten wurden. Im Jahr 2020 hat die Landesbeauftragte daher zahlreiche Verfahren geführt, um die jeweils Verantwortlichen dazu zu bringen, die von ihnen verantwortete Datenverarbeitung beim Betrieb ihrer Webseite mit den rechtlichen Vorgaben in Einklang zu bringen.

Ein **wiederkehrender Fehler** besteht darin, dass Verantwortliche in Bezug auf **einwilligungsbedürftige Cookies** auf ihren Webseiten – wenn überhaupt – lediglich auf deren Verwendung hinweisen, aber **keine vorherige wirksame Einwilligung durch aktives Tätigwerden** der Nutzerinnen und Nutzer vorsehen. Häufig werden nur sogenannte Cookie-Banner verwendet, die sich durch Nutzerinnen und Nutzer lediglich mit „OK“ oder ähnlich bestätigen lassen. Auch gibt es vereinzelt immer wieder Unklarheiten hinsichtlich der Frage, welche Datenverarbeitungsvorgänge einwilligungsbedürftig sind.

Neben einer Vielzahl an Verfahren, die aufgrund von Beschwerden angestoßen worden sind, haben wir gemeinsam mit den Aufsichtsbehörden anderer Bundesländer im Rahmen einer **koordinierten Prüfung den Sektor der hiesigen Online-Medien** anhand einer Auswahl Verantwortlicher einer Prüfung unterzogen. Nach Einleitung von Verfahren wurden teilweise bereits umfangreiche Änderungen an den Webseiten vorgenommen. Die Prüfergebnisse werden zurzeit ausgewertet.

Was ist zu tun?

Sofern Verantwortliche Cookies und ähnliche Technologien auf ihren Webseiten oder Smartphone-Anwendungen einsetzen wollen, die einwilligungsbedürftig sind, haben sie sicherzustellen, dass Nutzerinnen und Nutzer in diese Verarbeitung aktiv und wirksam einwilligen, bevor die Datenverarbeitung durchgeführt wird. Ein bloßer Hinweis – auch unter Verweis auf eine anderenorts mögliche Widerspruchsmöglichkeit – genügt bei einwilligungsbedürftigen Datenverarbeitungen nicht.

08

KERNPUNKTE

Digitale Arbeitswelten

IuK-Forschung

Transparenz und Usability

8 Modellprojekte und Studien

Das Unabhängige Landeszentrum für Datenschutz hat als Behörde der Landesbeauftragten für Datenschutz seine Aktivitäten in Initiativen im Bereich drittmittelfinanzierter Projekte und Studien fortgesetzt. Damit ist das ULD weiterhin im Bereich der Kooperation mit der Wissenschaft aktiv und erhält sich damit die Möglichkeit, proaktiv an der Erforschung datenschutzspezifischer Fragen und der Gestaltung einschlägiger Technologien und Lösungen mitzuwirken.

Im Berichtszeitraum wurden Projekte von der Europäischen Kommission und dem Bundesministerium für Bildung und Forschung (BMBF) gefördert. Beteiligungen an Projekten erfolgten weiterhin dort, wo entweder besondere datenschutzfördernde Lösungen (englisch: „Privacy-Enhancing Technologies“, kurz PETs) erforscht und entwickelt werden sollen oder wo besondere Risiken für die Rechte und Freiheiten natürlicher Personen bestehen.

Im Jahr 2020 beteiligte sich das ULD an Projekten zu aktuellen Themen in den Bereichen Privatheit und selbstbestimmtes Leben (Tz. 8.1), Datenschutz in digitalen Arbeitswelten (Tz. 8.2) sowie Datenschutz in der Technikforschung (Tz. 8.3) und setzt sein Engagement für Datenschutz, Transparenz- und Einwilligungsmanagement fort (Tz. 8.4).

8.1 Forum Privatheit

Wie schon in den vergangenen Jahren (zuletzt: 38. TB, Tz. 8.1) berichten wir von Fortschritten im interdisziplinären „Forum Privatheit“ zur Gewährleistung und Weiterentwicklung informationeller Selbstbestimmung und des Privaten in der digitalen Welt, das bereits im Dezember 2013 gestartet ist und bis März 2021 laufen wird. Das Projekt mit seiner „Think Tank“-Funktion hat den Fördermittelgeber, das BMBF, so sehr überzeugt, dass wir auch ab April 2021 zu dem Thema mit leicht verändertem Team und weitergeführten Projektideen weiterarbeiten können.

Forum Privatheit

Das „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt“ ist ein vom BMBF gefördertes interdisziplinäres Projekt, das sich mit Fragen des Datenschutzes, der Privatheit, der Selbstbestimmung und digitalen Grundrechten beschäftigt. Das Projekt bringt Wissenschaftlerinnen und Wissenschaftler aus Disziplinen wie Technik, Recht, Soziologie, Psychologie, Politologie, Wirtschaftswissenschaften und Ethik zusammen.

Das Schwerpunktthema des Vorjahres zu **Datenschutz in Schule und Kinderzimmer** mit der Jahreskonferenz im November 2019 erhielt in der Coronapandemie nur wenige Monate später mit Distanzlernen und Homeschooling eine verstärkte Relevanz.

Das Fokusthema für 2020: **„Selbstbestimmung und Privatheit – Gestaltungsoptionen für einen europäischen Weg“** passte besonders gut angesichts der EuGH-Entscheidung zum Privacy Shield (Tz. 2.5 und Tz. 11.5), aber auch internationale Entwicklungen in der Politik bis hin zu dem holprigen Abschied des Vereinigten Königreichs (UK) aus der Europäischen Union machten deutlich, dass sich die **Mitgliedstaaten der EU ihrer gemeinsamen Werte stärker bewusst** sein sollten und diese europäischen **Grundwerte und Grundrechte ein stabiles Fundament** sind, auf dem wir unsere Gesellschaft weiterentwickeln können. Mit einer simplen Kopie des Vorgehens in anderen internationalen Staaten – beispielsweise USA, Russland, China – können wir dies nicht erreichen, sondern es geht darum, den eigenen Weg zu finden und auszubauen. Die Datenschutz-Grundverordnung ist ein Baustein in diesem großen Puzzle des europäischen Wegs.

Dies alles hätte als umfangreiches Arbeitsprogramm für das Projektteam genügt, doch das alles **überlagernde Thema der Coronapandemie** prägte viele Diskussionen und Ausarbeitungen. Mit der Idee eines „Corona-Blogs“ konnten wir den Vorteil des Forums Privatheit – ein aufeinander eingespieltes interdisziplinäres Projektteam mit den

jeweiligen Perspektiven der Projektpartner im gesamten Bundesgebiet – nutzen: Darin befassten wir uns vor allem mit Konzepten, in denen **Infektionsschutz** ermöglicht wird, **ohne dabei Datenschutzanforderungen oder andere Grundrechte aufzugeben**.

https://corona.forum-privatheit.de/

Kurzlink: *https://uldsh.de/tb39-8-1a*

Im Mittelpunkt zahlreicher Beiträge stand das **Contact Tracing**, also die Möglichkeit einer Kontaktnachverfolgung im Infektionsfall, die ohne Standortdaten auskommt. In dem Corona-Blog konnten wir damit in Zusammenhang stehende Sachverhalte durchleuchten und Orientierungswissen für die interessierte Öffentlichkeit bereitstellen.

https://www.forum-privatheit.de/

Kurzlink: *https://uldsh.de/tb39-8-1b*

8.2 Projekt EMPRI-DEVOPS – Datenschutz in digitalen Arbeitswelten

Das Projekt **„Employee Privacy in Software Development and Operations“ (EMPRI-DEVOPS)** (38. TB, Tz. 8.3) beschäftigt sich seit November 2018 mit dem **datenschutzkonformen Einsatz von Softwaretools in zunehmend digitalisierten Arbeitswelten** (siehe auch Tz. 2.4). Projektziel ist die datenschutzkonforme Gestaltung von Softwareprodukten, die typischerweise im Kontext der agilen Softwareprogrammierung und der Systemadministration zum Einsatz kommen. Im Zuge der Coronapandemie und des dadurch bedingten Anstiegs von Heimarbeitsmodellen sind entsprechende Kooperationstools allerdings auch in anderen Branchen vermehrt verwendet worden.

Viele Unternehmen wurden in den letzten Monaten gewissermaßen dazu gezwungen, die Digitalisierung in der (Zusammen-)Arbeit stark zu beschleunigen, indem sie innerhalb kürzester Zeit auf Heimarbeit oder mobiles Arbeiten umsteigen mussten (siehe Tz. 6.3.3). Diese Entwicklung wurde in vielen Betrieben durch die Verwendung verschiedener Tools vorangetrieben, die den zeitnahen Austausch von Dokumenten oder eine gemeinsame Bearbeitung in Echtzeit ermöglichen. Diese **Kooperationstools** vereinfachen die Digitalisierung der bekannten Arbeitsvorgänge zum Teil enorm. Allerdings werden bei der Verwendung durch die Mitarbeitenden **Metadaten gespeichert, etwa Zeitpunkt und Nutzername beim Einloggen in ein Programm, bei jedem Erstellen, Ändern oder Speichern**.

Bei einer Untersuchung der Verwendung von solchen Zeitstempeln am Beispiel des Messengerdienstes Mattermost (vergleichbar mit Microsoft Teams oder Slack) haben die technischen Projektpartner von der Universität Hamburg u. a. festgestellt, dass personenbezogene bzw. personenbeziehbare Zeitstempel öfter gespeichert werden, als dies für das Funktionieren des Programms erforderlich wäre.

Metadaten

Metadaten sind strukturierte Daten, die Informationen über Merkmale und Eigenschaften anderer Daten enthalten. Bei Kooperationstools sind diese technisch erforderlich, um etwa bei gleichzeitiger Bearbeitung von Dokumenten die Reihenfolge von Änderungen nachzuvollziehen und Kollisionen zwischen Bearbeitungsständen aufzulösen. Ein Großteil der Metadaten ist personenbezogen.

Unabhängig von der Motivation für das Erfassen solcher Metadaten lassen sich aus diesen Rückschlüsse auf das Verhalten und die Leistung der Mitarbeitenden schließen, weshalb der **Einsatz dieser Tools regelmäßig dem Mitbestimmungsrecht des Betriebs- bzw. Personalrats unterfällt**. Schwierigkeiten ergeben sich für Mitarbeitende, wenn in der Organisation keine Beschäftigtenvertretung existiert. Ebenso fehlt es Freelancern, die nur auf Auftragsbasis tätig werden, aber dennoch oft zusammen mit internen Mitarbeitenden einer oder mehrerer Organisationen mittels solcher Tools zusammenarbeiten, an einem Schutz durch eine kollektive Interessenvertretung. Konkrete Vorgaben zum Datenschutz und zum Vorgehen bei der Einführung neuer Verfahren wären sowohl für die Mitarbeitenden als auch für die Arbeitgeber hilfreich. Gegenstand könnten etwa die Anforderungen und Prüfgegenstände sein, womit mittelbar Anreize für die Anbieter solcher Lösungen geschaffen würden, etwa **verständliche Dokumentation**

bereitzustellen, um den Verantwortlichen in seiner Kaufentscheidung und in der Einrichtung des Verfahrens zu unterstützen.

Inferenzrisiko

Ein Inferenzrisiko besteht, wenn sich aus vorhandenen Daten, etwa den bei der Nutzung von Kooperationstools anfallenden Metadaten, weitere sensible Informationen ableiten lassen. So können etwa Rückschlüsse auf Tagesabläufe und Arbeitsgewohnheiten aus Zeitstempeln der Aktivitäten (z. B. Bereitstellung von bearbeiteten Dokumenten) erlangt werden.

Auch wenn es für **Arbeitgeber** bei der Auswahl einer neuen Software nicht immer einfach ist, den Umfang der damit erhobenen (Meta-)Daten zu erkennen, kann er sich nicht dadurch herausreden, er hätte von der Datenverarbeitung nichts gewusst. Als **Verantwortlicher im Sinne der DSGVO** ist er dafür zuständig, dass die Vorgaben des Datenschutzrechts eingehalten werden. Legislativ wäre zu wünschen, dass klare Bestimmungen auch alle Beschäftigten schützen würden, für die kein Betriebsrat einstehen kann.

https://www.datenschutzzentrum.de/projekte/empri-devops/

Kurzlink: *https://uldsh.de/tb39-8-2*

Was ist zu tun?

Verantwortliche müssen ihre Verfahren beherrschen. Funktionsweise, Datenflüsse und Risiken müssen bekannt und dokumentiert sein, um eine fundierte Entscheidung über den Einsatz eines Verfahrens treffen zu können und um der Beschäftigtenvertretung eine Mitwirkung sinnvoll zu ermöglichen.

8.3 Projekt PANELFIT – Datenschutz und Ethik in der europäischen IuK-Forschung

Das von der EU-Kommission geförderte Projekt **„Participatory Approaches to a New Ethical and Legal Framework for ICT“ (PANELFIT)** (38. TB, Tz. 8.4.3) will dazu beitragen, dass Neuerungen durch die DSGVO schnell und vollständig von allen europäischen Akteuren im Bereich der Forschung zu Informations- und Kommunikationstechnologien (IuK) aufgegriffen und umgesetzt werden können. Während das Projekt auch ethische Fragen beleuchtet, konzentriert sich das ULD-Team auf Aspekte des Datenschutzes. Auf dieser Basis erarbeitet es Beiträge zu den **praxisorientierten Richtlinien**, die das PANELFIT-Projekt für in der Forschung Tätige zusammenstellt, und wirkt an den Empfehlungen für Entscheidungsträger wie z. B. Förderträger im Bereich der Informations- und Kommunikationstechnologien mit.

Im Jahr 2020 hat sich das PANELFIT-Projekt u. a. intensiv mit zwei Themen befasst, bei denen das ULD-Team größere Beiträge zugesteuert hat: Zum einen sind dies Praxisrichtlinien über die Konzepte des Datenschutzes für Forschende und Innovatoren. Zum anderen handelt es sich um eine kritische Analyse von Lücken und Problempunkten im derzeitigen europäischen Rechtsrahmen, die sich an politische Entscheidungsträger richtet.

Das ULD-Team hat zahlreiche grundlegende Abschnitte zu den Praxisrichtlinien beigetragen:

- eine Darstellung der DSGVO als Instrument zum Ausgleich des strukturellen Machtgefälles zwischen Verantwortlichen und Betroffenen,
- eine vertiefte Analyse der Prinzipien der DSGVO mit dazu passenden praktischen Maßnahmen zur Umsetzung,
- eine Ausarbeitung zur Dokumentation von Verarbeitungstätigkeiten,
- Hinweise zur Datenschutz-Folgenabschätzung,

- eine Analyse des Datenschutzes durch Technikgestaltung („by Design“) und datenschutzfreundliche Voreinstellungen („by Default“).

Im Weiteren wurden die Konzepte der **Pseudonymisierung und Anonymisierung** vertieft untersucht, da diese im Bereich der Forschung von besonderer Bedeutung sind. Im nächsten Schritt werden die Texte von externen Expertinnen und Experten begutachtet – insbesondere im Hinblick auf die Umsetzbarkeit für die Zielgruppe – und später in einer verbesserten Version in mehreren Sprachen zur Verfügung gestellt.

Für die kritische Analyse von Lücken und Problempunkten konnte das ULD auf die Arbeiten des Vorjahres zurückgreifen und hat sich vorwiegend mit dem Teilen von (pseudonymisierten) personenbezogenen Daten im wissenschaftlichen Bereich befasst. Eine Analyse des derzeit verfügbaren Informationsmaterials im Forschungsprogramm „Horizon 2020“ hat gezeigt, dass noch einige Lücken gefüllt werden können, um Forschende und Innovatoren dazu anzuleiten, zielgerichtet Lösungen für das datenschutzkonforme Teilen solcher Daten zu finden und einzusetzen. Im Weiteren hat das ULD-Team dokumentiert, warum eine **systematische und datenschutzkonforme Lösung für das Teilen personenbezogener Forschungsdaten** als „wissenschaftliches Gemeingut“ („Commons“) oder deren Kommerzialisierung in Europa notwendig ist und welche Kernelemente eine solche Lösung enthalten muss.

http://www.datenschutzzentrum.de/projekte/panelfit/

Kurzlink: *https://uldsh.de/tb39-8-3*

8.4 Projekte SPECIAL und TRAPEZE – Transparenz- und Einwilligungsmanagement für das semantische Netz

Das im September 2020 gestartete Projekt **„TRAnsparency, Privacy and security for European citiZEns“ (TRAPEZE)** wird von der EU-Kommission gefördert und schließt inhaltlich an das Projekt SPECIAL an (38. TB, Tz. 8.5). Eine europäische „Data Economy“ und ein einheitlicher Markt für Datentransfers sind dringend gewünscht – zumindest vonseiten der Wirtschaft und einiger öffentlicher Stellen. Die europäische Politik bekennt sich mit der „European Strategy for Data“ dazu und nennt dabei vorneweg richtigerweise Datenschutz, Grundrechte und Sicherheit als wichtige Eckpfeiler einer solchen Entwicklung.

Europäische Datenstrategie

Mit dem Dokument „Eine europäische Datenstrategie“ legte die Europäische Kommission einen Plan vor, wie die Nutzung personenbezogener und sonstiger Daten künftig aussehen kann, um diese für die wirtschaftliche Entwicklung und Forschung in Europa nutzbar zu machen. Datenschutz, Grundrechte und (Cyber-)Sicherheit werden darin zu Recht als zentrale Eckpfeiler genannt.

Als zentral für ein europäisches Modell der Datenökonomie werden dabei Konzepte und **Technologien** gesehen, die es den **Betroffenen ermöglichen, über die Verbreitung und Nutzung ihrer Daten selbstbestimmt zu entscheiden**. Zugleich sollen diese Lösungen den Austausch von Daten ermöglichen und die in Artikel 20 DSGVO geregelte Datenübertragbarkeit mit Leben füllen.

Im Projekt TRAPEZE haben sich Partner aus Forschung, Entwicklung, Industrie und öffentlichem Sektor mit dem ambitionierten Ziel zusammengefunden, den laufenden kulturellen Wandel beim Umgang mit Daten zu begleiten. Transparenz, rechtliche Compliance und das Konzept der Nutzerkontrolle sollen durch technische und organisatorische Lösungen sowie methodische Konzepte unterstützt werden. Betroffene sollen über eine **Dashboard-Anwendung** in die Lage versetzt werden, den komplexen Fluss ihrer Daten nachzuvollziehen und feinjustiert die Kontrolle über ihre Daten und deren Verwendung bei allen teilnehmenden Verantwortlichen zu übernehmen. Im Projekt wird dabei ein besonderer Schwerpunkt auf der **Usability** der Anwendung liegen, also auf der **Verständlichkeit der App und deren Funktionen**. Verständlichkeit von Informationen verkörpert den Datenschutzgrundsatz der Transparenz in besonderem Maße.

Einen grundlegenden Beitrag für eine solche Lösung stellt das unter dem Dach des World Wide Web Consortium (W3C) in kontinuierlicher Entwicklung befindliche **Vokabular zur Automatisierung** dar. Bereits das Vorgängerprojekt SPECIAL war an diesem Vorhaben wesentlich beteiligt, und das Projekt TRAPEZE wird weitere Impulse liefern.

Data Privacy Vocabularies and Controls Community Group

Die Gruppe befasst sich mit der Erarbeitung eines Vokabulars, das es gestattet, Aussagen zu Datennutzung, Inhalt und Umfang von Einwilligungen und Rechtsgrundlagen sowie weiterer Datenschutzaspekte computerlesbar und -auswertbar zu gestalten und diese Informationen beispielsweise zusammen mit den Daten abzulegen oder weiterzugeben. Dies bereitet z. B. die Grundlage für feingranulare Einwilligungs- und Berechtigungskonzepte mit der Möglichkeit für Rückfragen etwa zur Verarbeitung für weiter gehende Zwecke.

https://www.w3.org/community/dpvcg/

Kurzlink: *https://uldsh.de/tb39-8-4a*

Weiteres Standbein der im Projekt SPECIAL begründeten und nunmehr fortzuentwickelnden Lösung ist das **Konzept einer dynamischen Einwilligung (Dynamic Consent)**. Die Nutzung personenbezogener Daten für andere Verwendungszwecke oder eine Weitergabe an Dritte bedarf grundsätzlich einer Rechtsgrundlage und der Transparenz für die Betroffenen. Mittels Kommunikation mit den betroffenen Personen wird nicht nur die nötige Transparenz für eine Nachvollziehbarkeit hergestellt, sondern auch entweder die Einwilligung eingeholt bzw. aktualisiert oder aber eine bestehende gesetzliche Rechtsgrundlage kommuniziert. Betroffene werden damit in die Lage versetzt, von ihren Rechten Gebrauch zu machen.

https://www.datenschutzzentrum.de/projekte/trapeze/

Kurzlink: *https://uldsh.de/tb39-8-4b*

Was ist zu tun?

Der Weg in einen europäischen Datenmarkt birgt Risiken für Datenschutz und Grundrechte. Technologien für Datenaustausche und -verkäufe müssen Transparenz herstellen und Rechte der Betroffenen gewährleisten können.

09

KERNPUNKTE

Arbeitskreis Zertifizierung

Verwaltungsvereinbarung zwischen den Datenschutzbehörden

Akkreditierungskriterien

9 Zertifizierung und Akkreditierung

Auch im Berichtsjahr spielten Zertifizierung und Akkreditierung eine Rolle – leider immer noch nicht im Realeinsatz, sondern nun im Endspurt im AK Zertifizierung (Tz. 9.1) mit der Fertigstellung aller vorbereitender Dokumente und Vereinbarungen (Tz. 9.2, Tz. 9.3), damit deutschlandweit und EU-weit (Tz. 9.4) ein einheitliches Vorgehen garantiert wird. Dies beeinflusst auch die eigenen Planungen der Fortführung der Zertifizierung durch das ULD, wie dies vor der Geltung der Datenschutz-Grundverordnung durch Instrumente des Datenschutz-Gütesiegels und des Datenschutzaudits der Fall war (Tz. 9.5).

Eine Zertifizierung nach der Datenschutz-Grundverordnung dient dazu, die Datenschutzkonformität von Verarbeitungen personenbezogener Daten sichtbar zu machen. Solche Zertifizierungen können insbesondere sinnvoll sein, wenn Verantwortliche über die Wahl von Dienstleistern entscheiden sollen. Nicht nur eine erfolgreich durchlaufene Zertifizierung, sondern auch die dafür notwendige nachvollziehbare Dokumentation und die Prüfbarkeit der Verarbeitung werden einen großen Beitrag für die Rechenschaftspflicht der Verantwortlichen leisten. Die DSGVO beinhaltet einige Erleichterungen, wenn eine Zertifizierung vorgelegt werden kann.

9.1 Leitung des AK Zertifizierung

Seit drei Jahren leitet das ULD auf Wunsch der Datenschutzkonferenz (DSK) den Arbeitskreis (AK) Zertifizierung der Datenschutzaufsichtsbehörden in Deutschland. 2020 konnten durch die Arbeiten in dem Arbeitskreis sowohl die Verwaltungsvereinbarung zur deutschlandweiten Zusammenarbeit (Tz. 9.2) als auch die gemeinsamen Akkreditierungskriterien (Tz. 9.3) verabschiedet werden.

Eingebunden war stets auch die Deutsche Akkreditierungsstelle GmbH (DAkkS). Die DAkkS ist zwar in Deutschland für die Akkreditierung von Zertifizierungsstellen zuständig, doch die Aufsichtsbehörden werden bei der Begutachtung dieser Stellen tätig und sind maßgeblich an der Akkreditierungsentscheidung beteiligt. Auch gehört es zu den Aufgaben der Aufsichtsbehörden, die Zertifizierungskriterien zu genehmigen und die Befugnis zur Tätigkeit als Zertifizierungsstelle zu erteilen. Der AK Zertifizierung hat nun die Grundlage gelegt, dass diese Akkreditierungsverfahren starten können. 2020 wurden bereits in mehreren Bundesländern Anträge hierzu gestellt, wobei dies in Schleswig-Holstein bisher noch nicht der Fall ist.

Vorrangiges Ziel des AK Zertifizierung war es in der zweiten Jahreshälfte, **gemeinsame Kriterien für die Bewertung von Kriterienkatalogen** der Zertifizierungsstellen festzulegen. Die Arbeiten des dafür eingerichteten Unterarbeitskreises (UAK) Prüfkriterien waren Schwerpunkt in mehreren Sitzungen; es ist geplant, dass Anfang 2021 diese gemeinsamen Prüfkriterien der DSK vorgelegt werden können.

2020 fanden fünf Sitzungen des AK Zertifizierung statt, davon in Präsenz nur eine im Februar in Kiel.

Was ist zu tun?

Die Leitung des AK Zertifizierung durch das ULD wird auch 2021 fortgesetzt. Neben den gemeinsamen Prüfkriterien für Kriterienkataloge werden viele kleinere Themen wie die Ausgestaltung von Registern, Veröffentlichungen und die Koordinierung mit den Vorgaben der EU behandelt werden müssen.

9.2 Verwaltungsvereinbarung zwischen den deutschen Datenschutzbehörden

Anfang 2020 wurde zwischen allen Datenschutzaufsichtsbehörden in Deutschland (Länder und Bund) eine Verwaltungsvereinbarung zum Bereich Akkreditierung von Zertifizierungsstellen geschlossen. Nach Art. 57 Abs. 1 Buchst. q DSGVO haben die Aufsichtsbehörden die Aufgabe, Akkreditierungen von Zertifizierungsstellen gemäß Artikel 43 DSGVO vorzunehmen. Das bedeutet, dass alle Aufsichtsbehörden an der Akkreditierung von Zertifizierungsstellen mitwirken müssen. Diese Zertifizierungsstellen – in der Regel private Anbieter – wiederum zertifizieren Verantwortliche oder Auftragsverarbeiter hinsichtlich der Einhaltung der Vorgaben der DSGVO.

Die Akkreditierung selbst wird zwar durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) vorgenommen, jedoch sind die Aufsichtsbehörden als Gutachter eingebunden und entscheiden über die Akkreditierung mit. Insbesondere diese Zusammenarbeit zwischen den Aufsichtsbehörden und der DAkkS musste durch eine Vereinbarung geregelt werden. Diese beinhaltet grundsätzliche Regelungen der Zusammenarbeit sowie die Zusammensetzung von Gremien und stellt auch klar, dass Genehmigungen von Zertifizierungskriterien nach Art. 42 Abs. 5 DSGVO deutschlandweit gelten. Auch beinhaltet die Vereinbarung eine **Möglichkeit der gegenseitigen Unterstützung** und des freiwilligen Austauschs u. a. von Fachbegutachtenden, wenn aufgrund erhöhter Antragszahl personelle Engpässe in den Datenschutzbehörden einzelner Bundesländer entstehen. Dazu kommen Regelungen zur fortlaufenden Überwachung von Akkreditierungen.

Was ist zu tun?

Anträge auf Akkreditierung von Zertifizierungsstellen sind zu bearbeiten und zu entscheiden. Andere Bundesländer können gegebenenfalls in ihrer Arbeit unterstützt werden.

9.3 Akkreditierungskriterien veröffentlicht

Eine der Kernaufgaben des vom ULD geleiteten AK Zertifizierung im Jahr 2020 war es, zusammen mit den anderen deutschen Aufsichtsbehörden die zuvor erarbeiteten Kriterien gemäß Art. 64 Abs. 1 Buchst. c DSGVO für die Akkreditierung von Zertifizierungsstellen dem Europäischen Datenschutzausschuss zuzuleiten und die im Rahmen der Stellungnahme übermittelten Anpassungsvorschläge einzuarbeiten. Hierbei handelt es sich um Ergänzungen zur DIN EN ISO/IEC 17065 aus Datenschutzsicht. Dies konnte im abgelaufenen Berichtsjahr erfolgreich umgesetzt werden, sodass die von den deutschen Aufsichtsbehörden zusammen mit der Deutschen Akkreditierungsstelle (DAkkS) erarbeiteten Akkreditierungskriterien inzwischen das Stellungnahmeverfahren beim Europäischen Datenschutzausschuss erfolgreich durchlaufen haben. Diese Kriterien können nun im Rahmen von Akkreditierungsverfahren angewendet werden.

Unter anderem werden in den Kriterien Festlegungen getroffen, welche **Fachkundeanforderungen** eine Zertifizierungsstelle erfüllen muss, um Zertifizierungsverfahren kompetent durchführen zu können. Zudem werden spezielle **Verfahrensfragen und Publikationsanforderungen** geregelt.

Die aktuellen Akkreditierungsanforderungen können auf der Webseite der Datenschutzkonferenz abgerufen werden:

https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf

Kurzlink: *https://uldsh.de/tb39-9-3*

In diesem Zusammenhang ist das ULD neben anderen deutschen Datenschutzaufsichtsbehörden aktiv

im Unterarbeitskreis (UAK) Prüfkriterien eingebunden, der sich zur Aufgabe gemacht hat, einheitliche Anforderungen zu definieren, die es den deutschen Datenschutzaufsichtsbehörden erlauben, eingereichte Zertifizierungsprogramme auf einer einheitlichen Grundlage zu prüfen und zu bewerten. Hierzu wird vom UAK Prüfkriterien ein Dokument erstellt, das die Mindestanforderungen an solche Zertifizierungsprogramme skizziert. Die Arbeit des UAK Prüfkriterien ist dabei eng mit der Arbeit des AK Zertifizierung verzahnt.

Das erarbeitete Dokument soll nach der finalen Abstimmung im UAK Prüfkriterien und im AK Zertifizierung Anfang 2021 der DSK vorgelegt werden.

9.4 Mitwirkung in der europäischen Subgroup zur Zertifizierung

Das ULD war im Berichtszeitraum im Zusammenhang mit der Akkreditierung von Zertifizierungsstellen und mit der Zertifizierung in die Arbeit auf europäischer Ebene eingebunden.

Im Rahmen der „Compliance, e-Government und Health Subgroup (CEH ESG)“, einer Untergruppe des Europäischen Datenschutzausschusses, hat sich das ULD als Co-Berichterstatter u. a. an der Erarbeitung von **Stellungnahmen für Akkreditierungskriterien** von Zertifizierungsstellen nach Artikel 43 DSGVO in Verbindung mit § 39 BDSG aus anderen europäischen Mitgliedstaaten beteiligt.

Darüber hinaus wirkt das ULD zurzeit in der CEH ESG aktiv an der Erstellung von Kriterien zur Bewertung und Genehmigung von Zertifizierungsprogrammen mit (vergleichbar mit denen des UAK Prüfkriterien, Tz. 9.3).

Diese sollen es den europäischen Datenschutzaufsichtsbehörden erleichtern, die zur Genehmigung eingereichten Zertifizierungsprogramme bzw. -kriterien auf einer einheitlichen Basis und nach vergleichbaren Vorgaben zu prüfen und zu bewerten.

Was ist zu tun?

Die aktive Mitarbeit in den verantwortlichen Gremien auf europäischer Ebene soll weiter fortgeführt werden, um das Instrument der datenschutzrechtlichen Zertifizierung auf einer einheitlichen Basis weiter zu definieren und durch eine konsistente Anwendung und Umsetzung in Deutschland und Europa zu stärken.

9.5 Planung eigener Zertifizierungen des ULD

Das ULD hat bis Mai 2018 nach den damaligen Regelungen des LDSG Zertifizierungen in Form des Datenschutz-Gütesiegels Schleswig-Holstein durchgeführt. Auch nach den Regelungen der DSGVO kann das ULD Zertifizierungen vornehmen.

Aufgrund der guten Erfahrungen mit dem Datenschutz-Gütesiegel Schleswig-Holstein plant das ULD, dieses **in Zukunft wieder anzubieten**. Allerdings war für uns von Anfang an klar, dass wir uns vergleichbaren Regelungen unterwerfen wollen, wie sie für die privaten Anbieter von Zertifizierungen gelten – und die mussten erst ausgearbeitet werden. Mittlerweile stehen die endgültigen Akkreditierungskriterien für Deutschland fest (Tz. 9.3). Im Jahr 2021 werden die Prüfkriterien für Kriterienkataloge abgestimmt sein.

Frühestens dann können wir unseren eigenen Kriterienkatalog für eine ULD-Zertifizierung veröffentlichen. Dabei wird es sich im Gegensatz zum alten Datenschutz-Gütesiegel nicht um eine

Produktzertifizierung handeln. Entsprechend den Vorgaben der DSGVO stehen Verfahren, Prozesse und Dienstleistungen im Fokus. Zielgruppe der ULD-Zertifizierung werden öffentliche Stellen in Schleswig-Holstein sein. Im Gegensatz zu früher werden wir nicht mehr grundsätzlich auf anerkannte Sachverständige zurückgreifen. Auch die Gebühren für die Zertifizierung müssen noch festgesetzt werden.

Was ist zu tun?

Neben einigen Grundsatzfestlegungen muss insbesondere der Kriterienkatalog für die ULD-Zertifizierung ausgearbeitet und veröffentlicht werden. Die Gebühren und die genauen Verfahrensabläufe im Rahmen des eigenen Zertifizierungsprogramms müssen bestimmt werden.

10

KERNPUNKTE

Datenmanagement- und Datentreuhandsysteme

Schwärzen digitaler Dokumente

Zwang zur Cloud-Nutzung

Karteneinbindung in Webseiten

10 Aus dem IT-Labor

Vor langer Zeit gab es mal einen Raum in der Dienststelle des Landesbeauftragten für Datenschutz Schleswig-Holstein mit mehreren Computern: das IT-Labor. Dort wurden Datenverarbeitungen und IT-Systeme untersucht, typische Situationen nachgestellt und die damit verbundenen Risiken ermittelt, um dann wiederum die Wirkung und die Praktikabilität von bestimmten Maßnahmen auszutesten. Ein solches räumliches IT-Labor haben wir dank virtueller Maschinen und einer immer kleiner werdenden Hardware nicht mehr, aber wir beschäftigen uns weiterhin mit derartigen grundsätzlichen Fragen und Lösungen, die daher auch ein eigenes Kapitel im Tätigkeitsbericht haben.

In dem Berichtsjahr geht es um Risiken durch Bestätigungs-E-Mails (Tz. 10.1), Datenmanagement- und Datentreuhandsysteme (Tz. 10.2), korrektes Schwärzen digitaler Dokumente (Tz. 10.3), den Zwang zur Cloud-Nutzung (Tz. 10.4) und datenschutzkonformes Einbinden von Karten auf Webseiten (Tz. 10.5).

10.1 Praxisbericht: Bestätigungs-E-Mails bei Online-Formularen

In den letzten Jahren hat sich immer mehr durchgesetzt, dass Webseiten verschlüsselt aufgerufen werden. Erkennbar ist dies am verwendeten Protokoll HTTPS statt HTTP. In den meisten Browsern werden verschlüsselte Seiten auch mit einem Schlosssymbol o. Ä. als besonders sicher hervorgehoben. Beigetragen zu der Entwicklung haben eine erleichterte Einrichtung für Webserver, Initiativen wie „Let's encrypt“ (mit kostenfreier Bereitstellung von SSL/TLS-Zertifikaten) und nicht zuletzt die Bevorzugung verschlüsselter Webseiten in Suchmaschinen.

Besonders wichtig ist die Verschlüsselung, wenn auf einer Webseite auch **Daten von Nutzerinnen oder Nutzern in einem Formular abgefragt** werden – sei es beim Abo eines Newsletters, bei der Bestellung in einem Online-Shop oder gar bei der Online-Terminvergabe einer Arztpraxis (Tz. 4.5.2).

Da mit dem Versenden der eingegebenen Formulardaten mittels Webbrowser oft auch personenbezogene Daten und gegebenenfalls sogar besonders sensible Daten übertragen werden, ist eine **Verschlüsselung grundsätzlich notwendig und entspricht auch dem Stand der Technik**.

In der Praxis fällt aber immer wieder auf, dass die Vertraulichkeit der personenbezogenen **Daten nur in einer Richtung eingehalten** wird: Oft gehört zum Anmelde- oder Bestellprozess eine Bestätigung der eingegebenen Daten, die als E-Mail an die eingegebene E-Mail-Adresse geschickt wird. Meist sind in diesen Bestätigungs-E-Mails auch der eingegebene Formularinhalt oder andere Informationen zu der Person enthalten. Da jedoch diese E-Mails typischerweise nicht verschlüsselt verschickt werden, ist hier Vorsicht geboten: Durch eine unverschlüsselte E-Mail sind die versendeten Daten wiederum für Dritte einsehbar. Daher sollte beim Design solcher Systeme darauf geachtet werden, dass **mit solchen E-Mails keine sensiblen Daten übertragen** werden.

Beispielsweise können Inhaltsbestandteile ganz **weggelassen, gekürzt oder ausgeblendet** werden (z. B. nur einige Ziffern einer Kontoverbindung). Ebenso können andere Möglichkeiten eingerichtet werden, um die eingegebenen Daten – z. B. passwortgeschützt auf der verschlüsselt übertragenen Webseite – für Nutzerinnen und Nutzer einsehbar zu machen. Eine weitere Möglichkeit besteht darin, nach erfolgter Anmeldung bzw. Bestellung sofort **im Webbrowser eine Rückmeldung** zu geben, die dann ausgedruckt oder gespeichert werden kann.

Was ist zu tun?

Bei der Einrichtung von verschlüsselt übertragenen Webseitenformularen, bei denen nach dem Absenden eine Bestätigungs-E-Mail verschickt wird, ist darauf zu achten, dass mit einer solchen unverschlüsselt übertragenen E-Mail keine sensiblen Daten preisgegeben werden.

10.2 Datenmanagement- und Datentreuhandsysteme

Immer mehr Daten werden über jede einzelne Person verarbeitet – allein dies erschwert den Schutz jeder und jedes Einzelnen vor möglichem Missbrauch der Daten oder Fehlern in den IT-Systemen. Die von der Bundesregierung eingesetzte **Datenethikkommission** hat in ihrem Abschlussbericht 2019 darauf hingewiesen und u. a. gefordert, dass für einen umfassenden Schutz der Daten mehr Anstrengungen in die Forschung und Entwicklung von Datenmanagement- und Datentreuhandsystemen erfolgen müssten.

Voraussetzung für solche Systeme ist dabei, dass sie praxisgerecht und datenschutzkonform ausgestaltet sind. Für bereits vorhandene Angebote aus diesem Bereich fehlt bislang ein gemeinsames Verständnis. Die Fokusgruppe Datenschutz des Digital-Gipfels hat daher zum Digital-Gipfel 2020 ein Arbeitspapier vorgelegt, in dem Modelle dargestellt und erläutert und Einsatzszenarien konkretisiert werden.

Das Arbeitspapier ist unter dem folgenden Link abrufbar:

https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf?__blob=publicationFile&v=2

Kurzlink: *https://uldsh.de/tb39-10-2a*

Datenmanagementsysteme (auch: Personal Information Management System, PIMS) befinden sich noch in der Entwicklung und sind bisher nicht weit verbreitet. Die Entwicklungsansätze unterscheiden sich dabei sowohl im Hinblick auf die Herkunft der verwalteten Daten als auch bei der Speicherung und der Bereitstellung für Dritte: Einige Systeme agieren als Datencockpits, mit denen ein Überblick, Transparenz und Kontrolle der persönlichen Daten geschaffen werden sollen. Andere verwalten datenschutzrechtliche Einwilligungen, dienen als Datenschutzassistenten oder ermöglichen die Verwaltung digitaler Identitäten.

Personal Information Management System

Es gibt keine allgemeine Definition. Die verschiedenen Dienste und Systeme sollen Personen in die Lage versetzen, die Sammlung, Verarbeitung, Verbreitung sowie den Austausch ihrer persönlichen Daten zu kontrollieren. Ziel der Systeme ist typischerweise die Datensouveränität.

Datenmanagementsysteme können auch dazu dienen, **Pseudonyme zu verwalten** oder sicherzustellen, dass personenbezogene Daten nur in anonymisierter Form von Dritten verwendet werden können – indem beispielsweise personenbezogene Daten an forschende Dritte nur anonym bereitgestellt werden.

Dies spielte auch eine Rolle in unserer Zuarbeit zu der Veröffentlichung „Data Pseudonymisation: Advanced Techniques and Use Cases“ der European Union Agency for Cybersecurity (ENISA), in der **technische Methoden der Pseudonymisierung** im Sinne einer Risikoverringerung erläutert werden:

https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

Kurzlink: *https://uldsh.de/tb39-10-2b*

Datentreuhandsysteme können unterschiedliche Ziele verfolgen, die abhängig von den Daten und Einsatzszenarien sind. Ein typisches Ziel ist, dass eine datenverarbeitende Stelle (dies kann ein Verantwortlicher oder ein Auftragsverarbeiter sein) aus den von ihr verarbeiteten (gegebenenfalls pseudonymen oder pseudonymisierten) Daten keine Rückschlüsse auf eine natürliche Person ziehen können soll.

Datentreuhandsystem

Datentreuhänder stehen typischerweise in einer Vermittlerrolle zwischen verarbeitenden Stellen und Einzelpersonen. Sie sollen eine sichere Speicherung und Weitergabe von personenbezogenen Daten gewährleisten und übernehmen oft noch weitere Funktionen. Eine feststehende Definition hat sich auch hier noch nicht etabliert.

Ein Beispiel hierfür sind Lernmanagementsysteme, die personenbezogene Daten von Lernenden verarbeiten und auch Angebote Dritter (etwa weitere Lernplattformen) mit einbeziehen. Dabei werden diese Angebote so eingebunden, dass dort zwar individuelles Lernen möglich ist, die nicht erforderlichen Identitätsdaten aber gegenüber diesen Dritten nicht offengelegt werden müssen. Neben dem Schuleinsatz sind solche Konstellationen auch in der medizinischen Forschung oder im Bankwesen denkbar – dies zeigt die Bandbreite möglicher Einsätze.

Als übergeordnete Anforderungen an Datentreuhandsysteme wurden insbesondere Sicherheitsmaßnahmen und Transparenz herausgearbeitet. Empfohlen werden die Entwicklung einer Zertifizierung und eine Regulierung der Zulassung als Datentreuhänder. Beachtet werden müssen dabei branchenspezifische Anforderungen. Nicht zuletzt ist der Begriff „Treuhänder“ datenschutzrechtlich nicht eindeutig bestimmt und bedarf auch hier einer Konkretisierung.

Diese Themen spielten auch in dem **Rat für Informationsinfrastrukturen** eine Rolle, der sich ebenfalls mit unserer Beteiligung zu Datentreuhandstellen äußerte, um ein Augenmerk auf die Rolle von Wissenschaft und Forschung zu lenken:

http://www.rfii.de/download/rfii-stellungnahme-zu-datentreuhandstellen/

Kurzlink: *https://uldsh.de/tb39-10-2c*

All diese Initiativen werden sich weiter mit den Bedingungen beschäftigen, unter denen möglicherweise ein Datenteilen zu verschiedenen Zwecken realisiert werden kann und darf, wie dies auch in der **Europäischen Datenstrategie** (siehe auch Tz. 8.4) vorgesehen ist. Dabei kommt dem **Einhalten der Datenschutzanforderungen eine wesentliche Bedeutung** zu.

10.3 Unfallfreies Schwärzen digitaler Dokumente

Bei der Weitergabe von Dokumenten ist es wichtig, den Inhalt genau zu kontrollieren, insbesondere im Hinblick auf personenbezogene Daten. Informationen können in digitalen Dokumenten dabei nicht nur auf der Ebene der sichtbaren Daten vorliegen, sondern auch als **Metadaten**, die in der Datei gespeichert, aber bei der Darstellung des Dokumentes unsichtbar sind. Diese Informationen können vielfältig sein: Textdokumente enthalten dort oft Autorennnamen, Speicherpfade und Erstellungsdaten, andere Dateien wie Bilder enthalten mitunter sogar präzise GPS-Informationen über den Aufnahmeort. Gerade die Metadaten bergen das Risiko, dass unbewusst zu viele Informationen weitergegeben werden.

Um also sowohl sichtbare als auch unsichtbare Informationen zu entfernen, ist vor der Weitergabe digitaler Dokumente ein mehrschrittiges Vorgehen notwendig.

Zwar gibt es diverse Online-Tools zur Bearbeitung und Bereinigung digitaler Dokumente, doch die Tatsache, dass hier das möglicherweise sensible Ausgangsdokument einem in der Regel unbekannten externen Dienstleister im Web übermittelt werden muss, lässt Online-Tools für diese Aufgabe ausscheiden.

Zur Kontrolle der Metadaten sind spezielle Programme oder entsprechend spezialisierte Funktio-

nen der verwendeten Betrachtungssoftware nötig. Zu bedenken ist allerdings, dass einige der zum Entfernen ausgelobten Programme ihre Änderungen inkrementell vornehmen: Statt eine Information wirklich zu löschen, wird bei diesem Verfahren eine Markierung hinzugefügt, die **eine Information als gelöscht kennzeichnet** – etwa vergleichbar dem Abkleben eines Textes. Inkrementelle Verfahren sind dann von Vorteil, wenn die Möglichkeit der Rücknahme von Änderungen erwünscht ist. Im Falle der Löschung von Daten ist dies aber kontraproduktiv. Kommen also inkrementell arbeitende Werkzeuge zum Einsatz, muss das Dokument danach linearisiert werden: Durch diesen Prozess werden bis dahin **vorgenommene Änderungen fixiert** und eine Rücknahme unmöglich gemacht.

Auf der Inhaltsebene müssen unter Umständen Teile des sichtbaren Dokumentinhalts entfernt werden. Wie bei analogen Medien spricht man hier gemeinhin ebenfalls vom „Schwärzen“. Anders als in analogen Medien bedeutet „nicht mehr sichtbar“ im Digitalen allerdings nicht zwangsläufig „weg“, denn häufig werden wie bei der eben beschriebenen inkrementellen Änderung von Metadaten Inhalte lediglich überdeckt. Zudem bestehen einige Dokumente technisch gesehen aus Datenblöcken: einem Bild für die grafische Wiedergabe mit einem Anzeigeprogramm und einem nicht sichtbaren Teil, der die Buchstaben enthält, z. B. für eine Weiterverarbeitung per Textverarbeitung.

Das bloße Überlagern von Texten oder Bildern entfernt oft nicht die maschinenlesbare Information aus dem Dokument. Dies geschieht erst, wenn übereinanderliegende Ebenen miteinander verschmolzen werden, der schwarze Kasten und der darunterliegende Text also zu einer einzigen Pixelfläche werden (in der Papierwelt entspräche das dem Erzeugen einer Fotokopie zur Weitergabe). Darum bieten viele PDF-Bearbeitungsprogramme spezielle Schwärzungsfunktionen an, in denen im ersten Schritt Dokumentstellen markiert und diese dann in einem zweiten Schritt nachhaltig entfernt werden.

Ohne diesen finalen Schritt sind vorgenommene Abdeckungen reversibel. Aus diesem Grund ist das Schwärzen mit nicht speziell dafür vorgesehenen Programmen mitunter unzureichend: Wird die Schwärzung nur als Überlagerung ausgeführt, ist die fehlerhafte Funktion für Betrachtende zunächst nicht erkennbar. **Optisch sind die betreffenden Informationen unkenntlich. Dass der Text darunter maschinell extrahiert werden kann, ist weniger offensichtlich.**

Grundsätzlich muss bei der Weitergabe von Dokumenten auf alle Inhalte geachtet werden, die gegebenenfalls unerwünschte Rückschlüsse zulassen. Dies können **maschinell erzeugte Kennungen** sein wie „Yellow Dots“ (37. TB, Tz. 10.4), aber auch **zunächst unscheinbare Reste von Inhalten wie durchscheinende Buchstaben darunterliegender Dokumente, Wasserzeichen oder unzureichendes manuelles Redigieren im Weißbereich** (beispielsweise radierte Bleistiftvermerke). Insbesondere Dokumente, die im Entstehungsprozess vorübergehend in Papierform vorlagen und durch Einscannen oder Abfotografieren in eine digitale Form gebracht werden, sind prädestiniert für solcherlei **überschießende Informationen** – diese lassen sich in Bildbearbeitungsprogrammen oft **durch den Einsatz von Filtern oder Änderungen des Kontrastes sichtbar** machen.

Was ist zu tun?

Beim Schwärzen reicht es nicht, das Augenmerk allein auf Text und Bilder zu lenken, sondern alle Bereiche des Dokuments sind einer kritischen Prüfung zu unterziehen.

10.4 Alles in der Cloud

Einer der deutlichsten IT-Trends der letzten Jahre ist die **Verlagerung von Anwendungen in die Cloud**. Im Heimbereich bedeutet dies, dass immer weniger Daten auf den eigenen Geräten verbleiben, sondern beispielsweise aufgenommene Fotos – zumeist ohne bewusste Nutzerinteraktion – per Internet auf Server der Cloud-Anbieter übertragen werden. Dies verspricht einen hohen Komfortgewinn, da so die Fotos zeitnah auch auf anderen Geräten genutzt werden können, ohne wie in grauer Vorzeit mit Datenträgern hantieren zu müssen.

Auch andere Dateien lassen sich so einfach mit anderen austauschen, je nach Angebot auch gemeinsam bearbeiten. Ebenso müssen Medieninhalte wie Filme oder Musiktitel nicht erst heruntergeladen werden, sondern sind per Stream umfänglich verfügbar.

So werden **Speicherung, Verteilung und Nutzung von Anwendungen geräteunabhängig**. Ist der Akku des Tablets leer, kann man den eben begonnenen Film an der gleichen Stelle auf einem anderen Gerät weiter anschauen. Fällt das Handy versehentlich in einen Brunnen, bedarf es keines zu küssenden Frosches, der danach taucht, um weiter auf die aufgenommenen Fotos zugreifen zu können. Man hat ja alles noch in der Cloud.

Bei dieser Abstraktion wird allerdings übersehen, dass man selbst gar **nicht mehr die Verfügungshoheit über die eigenen Daten** hat. Oft ist den Nutzenden weder bewusst, wo ihre Daten denn nun eigentlich gespeichert werden, noch, wer darauf eigentlich alles Zugriff hat. Auch können viele Nutzende nicht sagen, welche Daten bei der Cloud-Nutzung anfallen, wie diese aggregiert und von wem zu welchen Zwecken ausgewertet werden. Zudem besteht die Gefahr, dass der Anbieter die Dienstleistung einstellt, sodass man womöglich gar keinen Zugriff mehr hat. Erst im letzten Jahr schaltete beispielsweise Microsoft den Zugriff auf gekaufte E-Books ab. Auch die wirtschaftliche Größe eines Anbieters bietet da keinen Schutz. Ist dies bei Medieninhalten vielleicht noch verschmerzbar, kann dies bei selbst erstellten Daten eine erhebliche Beeinträchtigung bedeuten.

Auch im Bereich der **Haustechnik** findet zusehends eine **Digitalisierung** statt. Nicht nur Heizung und Lampen lassen sich per Smartphone und App bedienen, Gegensprechanlagen mit Kameras können so aus der Ferne bedient werden, wenn sich jemand vor der eigenen Haustür befindet, man selbst sich aber nicht dahinter. Bei vielen dieser Angebote besteht das Problem, dass die Verbindung zwischen Hausgerät und Smartphone nicht direkt erfolgt, sondern einen Umweg über das Internet nimmt. So fallen bei jeder Steuerung von Licht und Wärme auch Daten bei den Anbietern dieser Lösungen an. Auch lässt sich dann auf die Steuerung nicht mehr zugreifen, wenn die Netzverbindung einmal ausfällt. Oft betreiben die Anbieter die für die Steuerung notwendigen Server allerdings gar nicht selbst, sondern nehmen dafür Angebote von Dritten in Anspruch. So sind im Bereich von Videoüberwachungslösungen mehrere Fälle bekannt geworden, bei denen der Zugriff auf die Bilddaten über Server in Asien lief und zudem **unzureichend abgesichert** war, sodass auch Unbefugte darauf zugreifen konnten.

Nicht nur Privatanwendende sehen sich indes mit diesem Trend konfrontiert. Auch in den IT-Umgebungen von Firmen, Schulen/Hochschulen, Kliniken usw. ist dies deutlich zu bemerken. Kritisch wird es, wenn die **Aktualisierung einer Anwendung plötzlich nicht mehr als On-Premise-Anwendung, die auf den eigenen Servern läuft, angeboten wird, sondern nur noch als Software as a Service (SaaS)**, sodass man einem Update, bei dem die eigenen Daten plötzlich außer Haus wandern, oft nur mit einer aufwendigen Migration auf ein anderes Produkt entkommen kann.

Denn zu bedenken ist bei so einer Umstellung nicht nur, dass man mit jeglicher Cloud-Nutzung plötzlich Dritten Zugriff auf die eigenen Daten und das jeweilige Nutzungsverhalten von – je nach Konstellation – Mitarbeitenden, Schülerinnen und Schülern, Patientinnen und Patienten usw. gewährt. Insbesondere wenn direkt oder indirekt Anbieter aus den USA beteiligt sind, ist dies nach dem Schrems-II-Urteil des EuGH (siehe auch Tz. 11.5) besonders kritisch zu betrachten.

Was ist zu tun?

Cloud-Dienstleistungen sollten immer eine Möglichkeit zum Export der Daten und zur anbieterunabhängigen Nutzung derselben bereitstellen.

Im Bereich der Heimautomation sollte auf Implementierungen geachtet werden, die von Internetanbindung und Herstellerservern unabhängig sind. Die Übertragung von Nutzungsdaten an die Hersteller muss jederzeit deaktivierbar sein.

Sind Anbieter aus den USA oder anderen Nicht-EU-Staaten an der Bereitstellung von Cloud-Diensten beteiligt, ist eine rechtskonforme Nutzung nur bei Vorliegen einer Rechtsgrundlage und ausreichender Datenschutzgarantien möglich und muss andernfalls unterbleiben.

In allen genannten Bereichen sind daher anbieterunabhängige Open-Source-Lösungen vorzuziehen, die mit offenen Standards arbeiten, wie es auch die IT-Strategie des Landes Schleswig-Holstein vorsieht.

10.5 Kartendienste auf Webseiten ohne Datenabfluss

Straßenpläne und Landkarten sind längst dem Faltplanalter entwachsen und liegen in vielfältigen digitalen Formen vor. Einige Anbieter haben dabei früh erkannt, dass die Nutzung digitaler Kartendienste mit einer Reihe spezieller Metadaten einhergeht. Oft wird die GPS-Position der abfragenden Person übermittelt, in jedem Fall jedoch das gesuchte Ziel. Bei mobilen Endgeräten fallen daneben oft auch Bewegungsdaten wie Beschleunigung und Geschwindigkeit an. Für Werbetreibende sind diese Zusatzinformationen interessant, weil sie deutlich über die sonst ermittelten Metadaten hinausgehen und damit zur Anreicherung von Profilen verwendet werden können.

Wer eine Webseite betreibt, möchte bisweilen seinen Gästen mit einem Lageplan die Anfahrts- oder Lieferwege verdeutlichen. Gleichzeitig ist es wichtig, Informationen der eigenen Gäste nicht ohne Grund an fremde Diensteanbieter weiterzureichen. Die Einbindung von Kartenmaterial in Form nachgeladener Inhalte birgt allerdings ebendieses Risiko. Rufen Nutzerinnen und Nutzer die Webseite mit eingebundener Landkarte auf, erfährt der Kartendienst neben IP- und Browserdaten mindestens auch die Geodaten des eingebundenen Kartenausschnitts. Wird das Kartenmaterial von Servern in außereuropäischen Drittstaaten geladen, kommt es daher zu einem **kritischen Datentransfer**: Nach dem Aus des Privacy-Shield-Abkommens (Tz. 11.5) fehlt in vielen Fällen eine Rechtsgrundlage, da solche Kartendienste meist in den USA ansässig sind. Hinzu kommt, dass die vermeintlich unerheblichen Daten in der Regel bei kommerziellen Anbietern landen, die sich selten nur auf das Gebiet der Kartendaten beschränken. Personenbezogene Daten, die im Rahmen des Kartendienstes an diese Anbieter übermittelt werden, landen also mitunter in einem Pool mit Daten zu einer Person, die der Anbieter aus anderen Quellen zu generieren imstande ist.

Beim Betrieb von Webseiten ist dieser Umstand stets im Auge zu behalten: Konkrete Daten der eigenen Gäste mögen irrelevant erscheinen, wenn man nur das eigene Webangebot betrachtet. Aber für Nutzende bleibt es selten beim Aufruf nur einer Webseite. Anbieter, die viele Besuche derselben Person über lange Zeit beobachten können, gewinnen hingegen auch **aus kleinen Datenschnipseln** ökonomisch wertvolle Zusatzinformationen und können **Profile erstellen**.

Um also Gäste der eigenen Webseite vor unnötigen Datentransfers zu schützen, sollte die Nutzung von Kartendaten unter dem Gesichtspunkt der **Datensparsamkeit** betrachtet werden. Die einfachste Möglichkeit der Einbindung von Kartenmaterial ist der **Screenshot**, also ein Bild der Kartendaten, das auf dem eigenen Server liegt. So eine Abbildung

erzeugt keinerlei Datenübertragung an Dritte. Allerdings ist zu beachten, dass nicht alle Anbieter von Kartendaten solch eine lokale Nutzung ihrer Materialien erlauben und so gegebenenfalls das Urheberrecht des Anbieters diesem Vorgehen entgegensteht – d. h., Webseitenbetreiber bei der Wahl solcher Anbieter also quasi „gezwungen“ wären, Inhalte zur Laufzeit nachzuladen. Stammen die **Daten aus freien Quellen wie z. B. Open-Data-Plattformen**, sind lokale Kopien im Allgemeinen kein Problem.

Sollen Gäste der Webseite Navigationsfunktionen nutzen können, können diese per Link eingebunden werden – in diesem Fall ist zur Nutzung eine aktive Handlung erforderlich. Die Verantwortung liegt dann beim Betreiber des Kartendienstes.

Kartenmaterial, das beim Aufruf der eigenen Webseite vom Diensteanbieter automatisch nachgeladen wird, birgt grundsätzlich das Risiko unerlaubter Datentransfers. Hier ist eine klare **Analyse der eingebundenen Dienste, ihrer Standorte und ihrer Datenschutzgarantien** vonnöten, um Datentransfers ohne Rechtsgrundlage auszuschließen. Neben einer gründlichen Dokumentation der Datentransfers in der eigenen Datenschutzerklärung ist auch eine klare **Information** der Webseitengäste erforderlich, bevor der Datentransfer erfolgt.

Was ist zu tun?

Kartendaten sollten in Form lokaler Abbildungen (Screenshot) in die eigene Webseite eingebunden werden, sofern Lizenzen oder Urheberrecht des genutzten Anbieters dem nicht entgegenstehen. Open-Data-Plattformen sind in dieser Hinsicht im Vorteil.

11

KERNPUNKTE

Leitlinien zu Targeting in sozialen Medien

Leitlinien zur Einwilligung

Konsequenzen aus dem EuGH-Urteil zum Privacy Shield

11 Europa und Internationales

Für einen effektiven Datenschutz in Europa ist eine möglichst einheitliche Auslegung und Anwendung der Datenschutz-Grundverordnung wesentlich. Aus diesem Grund erarbeitet und veröffentlicht der **Europäische Datenschutzausschuss (EDSA)**, das Gremium der Aufsichtsbehörden in Europa, Dokumente und Materialien, die wichtige Ergebnisse der Abstimmung unter den europäischen Aufsichtsbehörden enthalten. Die wesentliche Arbeit für solche Guidelines (Leitlinien) wird in den Arbeitsgruppen des **Ausschusses**, den Expert Subgroups, geleistet.

Diese war im Berichtsjahr natürlich stark von den datenschutzrechtlichen Herausforderungen und Problemen geprägt, die aufgrund des Auftretens der Pandemie seit dem Frühjahr 2020 entstanden sind. Vor allem die Positionierung des EDSA zu Fragen der Konzeption und – später – der länderübergreifenden Interoperabilität sogenannter **Contact Tracing Apps** war beherrschendes Thema im ersten Halbjahr 2020. Daneben konnten dennoch auch einige andere wichtige Themen bearbeitet werden.

Das ULD ist als Vertreter der Datenschutzaufsichtsbehörden der Länder Mitglied in der Key Provisions Expert Subgroup, die sich mit Grundsatzfragen beschäftigt. Als stellvertretender Ländervertreter ist das ULD in der Technology Expert Subgroup vertreten, die alle möglichen Aspekte zu Informations- und Kommunikationstechnologien und verwandten Themen in den Fokus nimmt. Weiterhin wirkt das ULD in thematisch passenden Unterarbeitsgruppen mit und entsendet zu Einzelfragen Vertreterinnen und Vertreter in die Arbeitsgruppen des EDSA.

Neben der regulären Arbeit als Mitglied in den Expert Subgroups, die u. a. darin besteht, die Interessen und Rechtsauffassungen der deutschen Aufsichtsbehörden der Länder einzubringen, beteiligten sich Mitarbeiterinnen und Mitarbeiter des ULD vereinzelt auch als (Co-)Berichterstatter.

Im Berichtsjahr betrifft die Arbeit auf europäischer Ebene insbesondere Fragen der Technikentwicklung zur Kontaktnachverfolgung in der Coronapandemie (Tz. 11.1), Targeting in sozialen Medien (Tz. 11.2), Grundsatzfragen zur Einwilligung (Tz. 11.3), Verarbeitung personenbezogener Daten in vernetzten Fahrzeugen (Tz. 11.4) und die Auswertung des EuGH-Urteils zum Privacy Shield sowie den Vorschlag der Europäischen Kommission zu Standarddatenschutzklauseln (Tz. 11.5). Daneben war das ULD zu Fragen der Zertifizierung und Akkreditierung eingebunden (Tz. 9.4). Unter Beteiligung des ULD wurden 2020 u. a. folgende Arbeiten abgeschlossen:

- Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications
- EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic – 14/04/2020
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
- Guidelines 05/2020 on consent under Regulation 2016/679
- Statement on the data protection impact of the interoperability of contact tracing apps – 16/06/2020
- Guidelines 08/2020 on the targeting of social media users – version for public consultation
- Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB – 19/11/2020

Abrufbar sind diese und andere Arbeiten des EDSA unter:

https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

Kurzlink: *https://uldsh.de/tb39-11-a*

https://edpb.europa.eu/other-documents_de

Kurzlink: *https://uldsh.de/tb39-11-b*

11.1 Guidelines aus Europa – datenschutzkonforme Kontaktnachverfolgung als Coronamaßnahme

Nachdem die Weltgesundheitsorganisation aufgrund der Verbreitung des Coronavirus SARS-CoV-2 und der COVID-19-Infektionen den Pandemiefall ausgerufen hatte, postulierten zahlreiche Politikerinnen und Politiker, dass es für geeignete Maßnahmen der Kontaktnachverfolgung erforderlich sei, alle verfügbaren Standort- und Bewegungsdaten der Menschen zu nutzen und darüber hinaus technisch weitere dieser Daten zu erheben. Parallel wurde mit der Arbeit an verschiedenen Apps begonnen, die Bausteine der Pandemiebekämpfung darstellen sollten.

Hinsichtlich sogenannter **Contact Tracing Apps** (wie z. B. der in Deutschland verwendeten Corona-Warn-App) haben die Datenschutzbehörden in mehreren Veröffentlichungen Stellung bezogen und Maßgaben und Empfehlungen erarbeitet, die bei Entwicklung und Betrieb solcher Apps zu berücksichtigen sind. Auf eine Anfrage der Europäischen Kommission hin hat der EDSA erste Empfehlungen ausgesprochen und u. a. den Standpunkt vertreten, dass die Nutzung einer Contact Tracing App auf freiwilliger Basis geschehen und zeitlich begrenzt sein müsse (Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic). Dieses Schreiben ist unter dem folgenden Link abrufbar:

https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-concerning-european-commissions-draft-guidance-apps_de

Kurzlink: *https://uldsh.de/tb39-11-3a*

In sehr kurzer Zeit erstellten die Aufsichtsbehörden unter maßgeblicher Beteiligung auch des ULD Leitlinien in Bezug auf Contact Tracing Apps, die im April 2020 als **„Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak"** vom EDSA veröffentlicht wurden. Darin bekräftigte der EDSA seine initialen Empfehlungen und hob u. a. hervor, dass Personen, die Contact Tracing Apps nicht nutzen möchten oder können, keine Nachteile entstehen dürfen. Außerdem wurde darauf hingewiesen, dass für Kontaktnachverfolgungs-Apps die Erfassung von **Standorten der einzelnen Nutzerinnen und Nutzer nicht erforderlich** ist und stattdessen Begegnungsdaten verwendet werden sollten. Ferner sollten Apps zur Kontaktnachverfolgung ohne eine direkte Identifizierung von Einzelpersonen funktionieren können und es sollten geeignete Maßnahmen getroffen werden, um eine Deanonymisierung zu verhindern. Die erhobenen Informationen sollten im Endgerät, beispielsweise im Smartphone der Nutzerin oder des Nutzers, verbleiben; es sollten lediglich die absolut notwendigen Informationen erhoben werden.

Der EDSA stellt abschließend klar, dass automatisierte Datenverarbeitung und digitale Technologien bei der Bekämpfung von COVID-19 zwar eine zentrale Rolle spielen können, jedoch zu gewährleisten ist, dass „jede unter diesen außergewöhnlichen Umständen ergriffene Maßnahme notwendig, zeitlich begrenzt und von minimaler Tragweite ist und einer regelmäßigen, konkreten Überprüfung sowie einer wissenschaftlichen Bewertung unterliegt". Der EDSA betont außerdem, „dass es **nicht** dazu kommen dürfe, **zwischen einer wirksamen Reaktion auf die derzeitige Krise und dem Schutz unserer Grundrechte wählen** zu müssen."

Die **„Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19"** sind unter dem folgenden Link abrufbar:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_de

Kurzlink: *https://uldsh.de/tb39-11-3b*

Die Anregung des EDSA, dass „ein gemeinsamer europäischer Ansatz ausgearbeitet oder zumindest ein interoperabler Rahmen geschaffen werden sollte", führte zu weiteren Fragen, die im Juni 2020 in der **„Erklärung über die Datenschutzfolgen der Interoperabilität von Kontaktnachverfolgungs-Apps"** aufgegriffen und stärker beleuchtet wurden:

https://edpb.europa.eu/our-work-tools/our-documents/other/statement-data-protection-impact-interoperability-contact-tracing_de

Kurzlink: *https://uldsh.de/tb39-11-3c*

Hervorzuheben ist die **konstruktive Hilfestellung** durch den EDSA, die in dieser außergewöhnlichen Situation in kurzer Zeit erarbeitet, abgestimmt und

veröffentlicht wurde. Auch wir haben uns hier mit juristischer und technischer Expertise im Sinne besonders datenschutzfreundlicher und vertrauenswürdiger Technikentwicklung eingebracht. Damit konnte Einfluss auf die Gestaltung von nationalen und europäischen Contact Tracing Apps genommen werden – ein den Datenschutz ignorierender Schnellschuss, wie er wohl einigen Politikerinnen und Politikern in vielen Ländern vorschwebte, konnte auf diese Weise zumindest in diesem Bereich vermieden werden.

11.2 Guidelines aus Europa – Targeting in sozialen Medien

Anfang 2018 wurde ein Datenskandal von riesigem Ausmaß aufgedeckt: Die Firma Cambridge Analytica hatte sich über eine vermeintlich wissenschaftliche App Zugang zu Daten Millionen von Facebook-Nutzerinnen und -Nutzern verschafft, darunter auch Ergebnisse von Persönlichkeitstests und Informationen zu den sozialen Beziehungen im Netzwerk. Diese Daten flossen in psychologische Profile ein und wurden u. a. für individualisierte Wahlwerbung genutzt. Die Firma erweckte den Eindruck, dass sie mit diesen sehr detaillierten Kenntnissen Wahlentscheidungen beeinflussen könnte. Wie groß der Effekt der **Manipulation der Menschen** tatsächlich war, ist zwar umstritten. Doch dass auf Personen zugeschnittene Werbung – beispielsweise durch geschicktes Anpassen und emotionale Trigger – vielfach funktioniert und Einfluss auf unsere demokratische Gesellschaft nehmen kann, ist nicht von der Hand zu weisen.

Aus diesem Grund beschloss die Artikel-29-Datenschutzgruppe, eine Social-Media-Arbeitsgruppe einzurichten, der das Mandat erteilt wurde, eine Leitlinie in Bezug auf das Targeting (gezielte werbliche Ansprache) von Social-Media-Nutzerinnen und -Nutzern auszuarbeiten. Unter **Berücksichtigung der Urteile des EuGH** in Sachen „Wirtschaftsakademie“, „Jehovas Zeugen“ und „Fashion ID“ ergaben sich viele Fragen, insbesondere zur Verteilung der Rollen und Verantwortlichkeiten zwischen einerseits den Social-Media-Plattformen, die Targeting-Funktionen anbieten, und andererseits Unternehmen oder anderen Organisationen, die diese Targeting-Funktionen nutzen.

Inhalt der **Leitlinien „Guidelines 08/2020 on the targeting of social media users“**, an deren Erarbeitung wir maßgeblich beteiligt waren, sind zahlreiche Fallbeispiele, die verdeutlichen, wie sich die **Verteilung von datenschutzrechtlicher Verantwortlichkeit** nach Ansicht des EDSA darstellt und welche Pflichten für die Beteiligten daraus resultieren. Auch wird erläutert, welche Rechtsgrundlagen unter welchen Bedingungen in typischen Konstellationen in Betracht kommen.

Die Leitlinien wurden im September vom Plenum verabschiedet. Daran schloss sich eine öffentliche Konsultation an. Die zahlreichen Rückmeldungen werden zurzeit ausgewertet, um sodann unter deren Berücksichtigung dem Plenum eine finale Version der Leitlinien vorlegen zu können.

Die zunächst nur in Englisch verfügbaren Guidelines sind unter dem folgenden Link abrufbar:

https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_de

Kurzlink: *https://uldsh.de/tb39-11-2*

11.3 Guidelines aus Europa – Überarbeitung und Ergänzung der Leitlinien zur Einwilligung

Unionsrechtliche Grundlage u. a. für die Verarbeitung personenbezogener Daten durch sogenannte Cookies ist die ePrivacy-Richtlinie (2002/58/EG, zuletzt geändert durch die sogenannte Cookie-Richtlinie 2009/136/EU). Anders als bei einer europäischen Verordnung (wie der DSGVO) verbleibt ein gewisser Spielraum bei der Umsetzung der Richtlinie durch die Mitgliedstaaten der Union. Um Konsistenz zwischen den aufsichtsbehördlichen Auffassungen und den darauf aufbauenden mitgliedstaatlichen Orientierungshilfen bezüglich der Verwendung von Cookies herzustellen, tauschen sich die Aufsichtsbehörden der Mitgliedstaaten auf Arbeitsebene fortlaufend aus und stimmen sich ab.

Erwägungsgrund 32 der DSGVO (Einwilligung)

Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist […] Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. […]

In diesem Zusammenhang wurden die Leitlinien zur Einwilligung **„Guidelines 05/2020 on consent under Regulation 2016/679“** überarbeitet und dabei vor allem klarstellende Ergänzungen vorgenommen: Bezüglich der Anforderungen an eine wirksame Einwilligung verweist die ePrivacy-Richtlinie auf das allgemeine Datenschutzrecht und damit nunmehr (seit deren Geltung, also ab dem 25.05.2018) auf die DSGVO. Insbesondere wurde durch die Ergänzungen in den Leitlinien klargestellt, dass das **bloße Weiternutzen einer Webseite nicht als wirksame Einwilligung angesehen** werden kann, weil eine solche Aktivität unter keinen Umständen dem Erfordernis einer klaren und bestätigenden Handlung genügt.

Die (aktualisierten) Leitlinien sind unter dem folgenden Link abrufbar:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de

Kurzlink: *https://uldsh.de/tb39-11-3*

11.4 Guidelines aus Europa – vernetzte Fahrzeuge und Mobilitätsanwendungen

Die Nutzung heutiger Autos ist kaum noch möglich, ohne dass eine Vielzahl an personenbezogenen Daten verarbeitet wird. Infotainment-, Verkehrsinformations- und diverse Fahrassistenzsysteme gehören mittlerweile nicht nur in Oberklassemodellen zur Ausstattung. Rund um heutige Autos hat sich daher ein komplexes Ökosystem gebildet. In vielen Modellen, die in den letzten Jahren auf den Markt gekommen sind, sind Sensoren und vernetzte Bordgeräte integriert, die u. a. die Motorleistung, die Fahrgewohnheiten, die besuchten Orte oder auch biometrische Daten der Fahrerinnen und Fahrer zu Authentifizierungs- oder Identifizierungszwecken sammeln und aufzeichnen können.

Um in diesem komplexen Bereich Orientierung zu geben, beschäftigt sich der EDSA in den Leitlinien mit diesem Ökosystem und konzentriert sich dabei insbesondere auf die **Verarbeitung personenbezogener Daten betroffener Personen** (z. B. Fahrerinnen und Fahrer, Passagiere, Fahrzeugbesitzerinnen und -besitzer, Mieterinnen und Mieter usw.), die **innerhalb des Fahrzeugs** verarbeitet, **zwischen dem Fahrzeug und den damit verbundenen persönlichen Endgeräten** (wie z. B. einem Smartphone oder Navigationsgerät) ausgetauscht oder innerhalb des Fahrzeugs gesammelt und **an externe Stellen zur weiteren Verarbeitung exportiert** werden (z. B. an Fahrzeughersteller, Infrastrukturbetreiber, Versicherungen oder Autowerkstätten).

Die Leitlinien befanden sich in der öffentlichen Konsultation. Eine überarbeitete Version wird aller Voraussicht nach im ersten Quartal 2021 verabschiedet werden. Abrufbar sind die Leitlinien **„Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications“** (bisher nur in Englisch) hier:

https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_de

Kurzlink: *https://uldsh.de/tb39-11-4a*

Da es sich bei vernetzten Fahrzeugen um funkfähige Systeme handelt, können sie passiv geortet werden, z. B. per **WLAN- oder Bluetooth-Tracking**.

In diesem Sinne unterscheiden sie sich nicht von anderen verbundenen Endgeräten. Die Leitlinien beschäftigen sich nicht im Detail mit dieser Frage, weisen jedoch ausdrücklich auf diesen Problembereich hin und verlinken zur Arbeit des ULD, da wir uns etwas eingehender damit beschäftigt haben:

https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html

Kurzlink: *https://uldsh.de/tb39-11-4b*

11.5 Technische und vertragliche Empfehlungen bei Drittstaatentransfers

Im **Urteil des EuGH zur Rechtssache C-311/18 („Schrems II“)** zu Datenübertragungen in die USA wurde festgestellt, dass neben dem für ungültig erklärten **Privacy Shield** auch die **Nutzung der von der EU genehmigten Standarddatenschutzklauseln** (auch teilweise als Standardvertragsklauseln bezeichnet) gegebenenfalls nicht ohne Weiteres ausreicht, um eine Datenübermittlung in die USA zu legitimieren.

Diese Feststellung des Gerichts ist **konsequent** – gehörten doch zu den wesentlichen Kritikpunkten des EuGH Art und Umfang staatlicher Zugriffe, beispielsweise durch Geheimdienste, und mangelnde Rechtsschutzmöglichkeiten für die Betroffenen. Dass vertragliche Regelungen zwischen Datenverarbeitern auf solche Zugriffe nur wenig Einflussmöglichkeiten haben, leuchtet ein und war auch schon bei der ersten Entscheidung des EUGH zu Datenübermittlungen in die USA im „Safe Harbor“-Urteil problematisiert worden (36. TB, Tz. 11.1).

Dennoch hängt es von den genauen Umständen ab, ob durch eine Datenübermittlung in einen Drittstaat (d. h. in einen Staat außerhalb des örtlichen Geltungsbereichs der DSGVO) ein **unvertretbares Risiko** entsteht. Dazu hat der Europäische Datenschutzausschuss (EDSA) (38. TB, Tz. 11) Empfehlungen herausgegeben, mit denen Verantwortliche prüfen können, unter welchen Voraussetzungen eine solche Übermittlung möglich ist. Diese Empfehlungen **„Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data“** sind hier abrufbar:

https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_de

Kurzlink: *https://uldsh.de/tb39-11-5a*

Die Empfehlungen beschränken sich nicht auf die USA. Einer der Kernpunkte ist die **Analyse der rechtlichen Situation einschließlich der praktischen Umsetzung im Empfängerland**, um das dortige Datenschutzniveau einzuschätzen. Einen zweiten Kernpunkt bilden **zusätzliche Maßnahmen, mit denen durch (vertragliche) Ergänzungen (sogenannnte „Supplementary Measures“) das Datenschutzniveau gegebenenfalls so weit angehoben** werden kann, dass es den europäischen Vorgaben entspricht.

Dies erscheint zunächst widersinnig: Warum sollte eine vertragliche Bindung unbefugte Datenzugriffe durch Behörden im Empfängerland verhindern können? Bei näherem Hinsehen gibt es jedoch bedenkenswerte Aspekte: Nicht jedes Unterschreiten des europäischen Datenschutzniveaus beruht auf unbefugten staatlichen Zugriffen, sondern kann u. a. auch aus mangelnden datenschutzrechtlichen Regelungen, etwa zu Betroffenenrechten (z. B. Löschung, Auskunft, Berichtigung) oder zu Transparenz- und Dokumentationsverpflichtungen, resultieren. Diese lassen sich vertraglich ergänzen.

Daneben können in einigen Fällen technische Maßnahmen zum Einsatz kommen, mit denen sich unbefugte Zugriffe technisch unterbinden lassen. Typische Beispiele sind Verschlüsselungsverfahren, die wirksame Pseudonymisierung von Daten oder eine geteilte Verarbeitung. Auf diese Weise entsteht im besten Fall erst gar keine tatsächliche Möglichkeit eines unbefugten Zugriffs. In anderen Fällen, wenn beispielsweise die Verarbeitung von personenbezogenen Klartextdaten der Geschäftszweck ist, etwa bei Kommunikationsdiensten oder Servicediensten („Helpline“), sind bisher keine technischen Maßnahmen verfügbar.

Bis Ende 2020 befanden sich diese Empfehlungen in einer Konsultationsphase, sodass in Kürze möglicherweise Ergänzungen vorgenommen werden.

Parallel beschäftigt sich der EDSA mit **überarbeiteten Standarddatenschutzklauseln, die von der Europäischen Kommission im Entwurf vorgelegt**

wurden. Dies wird vom EDSA generell begrüßt, dennoch werden vonseiten der Datenschutzaufsichtsbehörden in Europa Verbesserungen gefordert:

https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_de

Kurzlink: *https://uldsh.de/tb39-11-5b*

Was ist zu tun?

Verantwortliche oder Auftragsverarbeiter, die bisher Daten auf Basis des Privacy Shield oder der Standarddatenschutzklauseln in die USA übertragen haben, müssen eine valide Rechtsgrundlage vorweisen können. Sie sollten mithilfe der von den Aufsichtsbehörden veröffentlichten Empfehlungen überprüfen, ob der bisherige Datentransfer auf vertraglicher Basis möglich ist oder ob die Datenverarbeitung im Sinne einer Rechtskonformität zu verändern ist. Datenexporteure sind verpflichtet, die Datenübermittlung auszusetzen oder zu beenden, wenn der Schutz der übermittelten Daten auch durch zusätzliche Maßnahmen nicht hinreichend sichergestellt werden kann.

12

KERNPUNKTE

Anpassung des IZG-SH notwendig

TOP 5 der Beschwerden

Informationspflicht privater Stellen

12 Informationsfreiheit

Jede natürliche und juristische Person hat das Recht, insbesondere bei Behörden vorhandene Informationen abzufragen. Dies dient der Transparenz staatlichen Handelns und ist in Schleswig-Holstein seit 2012 gesetzlich geregelt. Leider steht weiterhin eine Anpassung des aktuellen Informationszugangsgesetzes (IZG-SH) an die 2018 erfolgten Änderungen des LDSG aus (Tz. 12.1).

Das ULD kann von Petentinnen und Petenten vermittelnd eingebunden werden, wenn diese der Meinung sind, dass ihr Antrag nach dem IZG-SH unrechtmäßig beantwortet (oder gar nicht darauf reagiert) wurde. Die Top 5 der Beschwerden im Berichtszeitraum haben wir zusammengefasst (Tz. 12.2).

Einige besondere Fälle im Berichtsjahr haben wir herausgegriffen, so die Informationspflicht privater Stellen (Tz. 12.3), die Antragstellung im Betreuungsverhältnis (Tz. 12.4), Einsicht in Klausuraufgaben (Tz. 12.5) und den Begriff des Betriebs- und Geschäftsgeheimnisses (Tz. 12.6). Schließlich gehen wir auch noch auf die Transparenz und den Pottkieker-Gesetzentwurf (Tz. 12.7) ein.

12.1 Weiterhin Anpassung des IZG-SH an LDSG und DSGVO notwendig

Schon im vorletzten Tätigkeitsbericht haben wir darauf hingewiesen, dass das Informationszugangsgesetz Schleswig-Holstein (IZG-SH) geändert werden muss (37. TB, Tz. 12.1). Die Rolle des ULD im Bereich der Informationsfreiheit ist beratender Art und besteht insbesondere in einer **Mediation zwischen den Interessen der Petentinnen bzw. Petenten und den Behörden**. Im Gegensatz dazu tritt im Bereich der Datenschutzaufsicht, wie sie LDSG und DSGVO im Fokus haben, statt dieses Vermittlungsgedankens der aufsichtsbehördliche Charakter deutlich in den Vordergrund. Dennoch verweist die jetzige Version des IZG-SH bei den Befugnissen des ULD auf die Regelungen des LDSG in Verbindung mit der DSGVO. **Dies ist vermutlich bei der Novellierung des LDSG Anfang 2018 übersehen worden.** Die dort geregelten Anweisungs- und Anordnungsbefugnisse des ULD können nicht auf diese vermittelnde Form des Petitionsrechts übertragen werden. Daher plädieren wir dafür, in das IZG-SH angepasste Aufgaben und Befugnisse des ULD aufzunehmen, wie es auch in anderen Bundesländern (u. a. Brandenburg, Nordrhein-Westfalen und Thüringen) der Fall ist. Entsprechende Vorschläge haben wir auch schon dem Innen- und Rechtsausschuss des Landtages aufgezeigt.

Was ist zu tun?

Das IZG-SH ist anzupassen.

12.2 Top 5 der Beschwerden von Petentinnen und Petenten

Im Berichtszeitraum haben uns etwa 50 Anfragen von Petentinnen und Petenten erreicht, die sich über eine unzureichende Beantwortung ihrer Anfragen nach dem IZG-SH beschwert haben. Insbesondere im Zeitraum zwischen März und Juni 2020 kam es aufgrund der Homeoffice-Regelungen in Teilen der öffentlichen Verwaltung zu Verzögerungen bei der Bearbeitung von IZG-SH-Anfragen der Bürger. Aber auch auf Rückfragen des ULD wurde mehrfach um Fristverlängerung gebeten, u. a. mit der Begründung, Kolleginnen und Kollegen nicht zu erreichen bzw. keinen Fernzugriff auf die Daten zu haben.

Hier unsere Top 5 der Beschwerden der Petentinnen und Petenten im Bereich des IZG-SH:

1. Keine Antwort

Der Klassiker ist weiterhin, dass auf Anträge gar nicht geantwortet wird. Auch wenn die Kenntnisse bei den Behörden zum IZG-SH und den damit verbundenen Rechten auf Zugang zu Informationen nach unserer Beobachtung von Jahr zu Jahr zunimmt, so gibt es immer noch Stellen, bei denen diesbezüglich Grundlagenarbeit geleistet werden muss. Insbesondere Anfragen per E-Mail werden teilweise ignoriert. Allerdings wird in der Regel auf unsere Aufklärung hin zeitnah entweder das Gespräch gesucht oder die Informationen werden rausgegeben.

2. Kein Bescheid im Fall einer Ablehnung

Eng verwandt mit dem ersten Punkt ist, dass öfter bei Ablehnungen kein ordentlicher Bescheid nach § 6 IZG-SH erlassen wird. Teilweise wird nur mit einer formlosen E-Mail über die Nichtübermittlung der angefragten Informationen informiert, ohne auf die Rechtsschutzmöglichkeiten nach § 6 Abs. 4 IZG-SH hinzuweisen. Dies hat für die Behörde allerdings sogar den Nachteil, dass dann die Fristen deutlich verlängert werden. Es zeigt aber insbesondere, dass nicht immer bei den informationspflichtigen Stellen erkannt wird, dass es sich bei Anträgen um solche nach dem IZG-SH handelt bzw. diese entsprechend auszulegen wären. Die Antragstellerin bzw. der Antragsteller ist nicht in der Pflicht, ausdrücklich auf das IZG-SH hinzuweisen. Es ist Aufgabe der Behörde, im Zweifel von einem Antrag im Sinne des IZG-SH auszugehen oder zumindest diesbezüglich noch einmal bei der Antragstellerin bzw. dem Antragsteller nachzufragen.

3. Gebühren

Mehrfacher Streitpunkt waren die Gebühren, die angefragte Behörden den Antragstellerinnen und Antragstellern für die Auskunft auferlegten. Geregelt ist dieses in einer Kostenverordnung des Landes (GVOBl. Schl.-H. 2007, 225). Danach können für umfassende Auskünfte Gebühren bis 250 Euro und für außergewöhnlich aufwendige Auskünfte Gebühren bis 500 Euro erhoben werden. Für einfache Auskünfte mit einem Aufwand von einer halben bis dreiviertel Stunde gehen wir davon aus, dass keine Gebühren erhoben werden. Dabei ist zu beachten, dass das grundsätzliche Einarbeiten in den Themenbereich der Informationsfreiheit nicht zum anzusetzenden Verwaltungsaufwand hinzugerechnet werden darf, was auch entsprechende Rückfragen bei uns umfasst. Die bzw. der Anfragende soll nicht durch übermäßige Gebühren von ihrem bzw. seinem Recht auf Informationszugang abgehalten werden.

In den meisten uns vorgelegten Fällen wurden die Gebühren von der Behörde vorab der bzw. dem Anfragenden mitgeteilt, sodass die Möglichkeit bestand, den Antrag noch kostenfrei zurückzunehmen. Teilweise konnten wir erreichen, dass die Gebühren reduziert wurden.

4. Fehlende Abwägung

Bei den Ablehnungsgründen wurde besonders oft auf das Vorliegen personenbezogener Daten im Sinne des § 10 Nr. 1 IZG-SH verwiesen. Mehrfach ließen es die Behörden jedoch mit dieser Begründung bewenden. Weder wurde dabei abgewogen, ob die schutzwürdigen privaten Interessen an der Geheimhaltung gegenüber dem öffentlichen Bekanntgabeinteresse überwiegen, noch wurden die Betroffenen um Einwilligung zur Weitergabe der Informationen angefragt. Auch fehlten mehrfach Aussagen darüber, ob tatsächlich alle angefragten Informationen Personenbezug aufwiesen oder zumindest Teile hätten herausgegeben werden können.

Auf unsere Vermittlung hin wurden die notwendigen Abwägungen und Nachfragen bei den Betroffenen zur möglichen Einwilligung in die Weitergabe der Informationen nachgeholt. Manchmal ergaben sich hieraus doch Möglichkeiten, um zumindest teilweise den Anfragen zu entsprechen. Einen besonderen Schwerpunkt in diesem Bereich bildeten Anfragen zur Einsicht in Bauakten, wobei gerade bei diesen meist nur schwerlich Informationen ohne Personenbezug abgetrennt werden können.

5. Angenommene Missbräuchlichkeit

Außerdem wurden Überlegungen von Behörden an uns herangetragen, ob Anfragen wegen offensichtlicher Missbräuchlichkeit nach § 9 Abs. 2 Nr. 1 IZG-SH abgelehnt werden können. Wir haben dann erklärt, dass dieses nur in besonders gelagerten Fällen anzunehmen ist und eine hohe Hürde besteht, bevor von Missbrauch ausgegangen werden kann. Insbesondere sind mehrfache Anfragen zu unterschiedlichen Themen kein Grund, Missbrauch anzunehmen. Vielmehr muss in der Regel

erkennbar sein, dass Anträge nur deshalb gestellt werden, um Behörden in ihrer Funktionsfähigkeit zu stören. Entsprechende Aussagen der Anfragenden oder auch Mehrfachanfragen zum selben Sachverhalt durch dieselbe Person können Indizien hierfür sein. Im Zweifel wird der Missbrauch jedoch abzulehnen sein und die Anfrage ist zu bearbeiten.

Was ist zu tun?

Die informationspflichtigen Stellen müssen sich stärker über ihre Rechte und Pflichten bei der Bearbeitung von Anträgen nach dem IZG-SH bewusst werden. Hierzu stellt das ULD Informationsmaterial zur Verfügung, das regelmäßig überarbeitet wird. Auch stehen wir gerne für Fragen zur Verfügung.

12.3 Informationspflicht privater Stellen

Im Jahr 2020 erreichten uns mehrere Anfragen, in denen Bürgerinnen und Bürger Informationen von privaten Stellen nach dem IZG-SH wünschten, diese jedoch teilweise aufgrund der privatrechtlichen Organisation abgelehnt wurden. Dies betraf u. a. juristische Personen des Privatrechts im Bereich öffentlicher Nahverkehr. Diese sind in § 2 Abs. 3 Nr. 2 IZG-SH auch ausdrücklich als Beispiel für informationspflichtige Stellen genannt. Allerdings muss hinzukommen, dass sie Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handlungsformen des öffentlichen Rechts übertragen bekommen haben. Im Gegensatz zur früheren Rechtslage in Schleswig-Holstein ist damit inzwischen eine Beleihung im Sinne des § 24 Landesverwaltungsgesetz gemeint.

Es zeigte sich, dass einige der angefragten Stellen **nicht eindeutig beantworten** konnten, ob eine solche Übertragung von Aufgaben der öffentlichen Verwaltung tatsächlich erfolgt ist. In einem Fall konnte auch die Behörde, die die private Stelle beauftragt hatte, erst nach längerer Recherche hierzu eine Antwort geben.

Beleihung

Nach § 24 Landesverwaltungsgesetz können natürlichen und juristischen Personen des Privatrechts sowie nichtrechtsfähigen Vereinigungen Aufgaben der öffentlichen Verwaltung zur Erledigung in den Handlungsformen des öffentlichen Rechts nur durch Gesetz oder aufgrund eines Gesetzes übertragen werden. Dies ist u. a. nur möglich, wenn die Zuständigkeit der Behörde nicht ausdrücklich vorgeschrieben ist und auch die Eigenart der Aufgabe dem nicht entgegensteht.

Was ist zu tun?

Wenn private Stellen Aufgaben der öffentlichen Verwaltung übertragen bekommen, sollte klargestellt werden, ob es sich um eine Übertragung nach § 24 Landesverwaltungsgesetz handelt. Dann sollte die übertragende Behörde der privaten Stelle auch mitteilen, dass sie den Regelungen des IZG-SH unterliegt und entsprechende Prozesse zur Herausgabe angefragter Informationen gemäß den gesetzlichen Anforderungen einrichtet.

12.4 Antragstellung im Betreuungsverhältnis

In einem Fall war der Antrag auf Informationszugang einer in einem Betreuungsverhältnis stehenden Person mit der Begründung abgelehnt worden, dass deren Betreuungsausweis mit dem Eintrag „Vertretung gegenüber Behörden“ versehen war. Bei dem Anspruch nach § 3 IZG-SH handelt es sich jedoch um einen **rein rechtlichen Vorteil** und rechtliche oder wirtschaftliche Nachteile sind bei der Geltendmachung des Anspruchs nicht erkennbar, sodass es auch nicht auf die Geschäftsfähigkeit der antragstellenden Person ankommt.

Auch stellt die Angabe „Vertretung gegenüber Behörden“ keine eigenständige Regelung des Betreuungsverhältnisses dar, sondern dient lediglich der Klarstellung der Vertretungsberechtigung der Betreuerin bzw. des Betreuers im Rahmen eines zugleich übertragenen Aufgabenkreises.

Die Behörde musste den Antrag bearbeiten, was sie nach unserem Hinweis auch tat.

12.5 Einsicht in Klausuraufgaben

Ein Petent wünschte vergangene Prüfungsaufgaben einzusehen. Das Prüfungsamt lehnte die Herausgabe der Aufgaben insbesondere mit der Begründung ab, dass dieses die Ausbildung der Prüflinge beeinträchtigen würde, da sich Aufgaben fachspezifisch wiederholen würden. Wir kamen zu dem Ergebnis, dass hier eine bestehende Prüfungsordnung mit ihren Regelungen zur Einsicht dem IZG-SH vorgeht.

Aber selbst wenn man dieses nicht annahm, konnte der Antrag unserer Einschätzung nach abgelehnt werden. Dem geltend gemachten Anspruch stand in diesem Fall zumindest § 9 Abs. 1 Satz 1 Nr. 3 IZG-SH entgegen. So könnte der behördliche Entscheidungsprozess nachhaltig durch die Bekanntgabe der begehrten Unterlagen gestört werden. Zu berücksichtigen war auch, dass gemäß § 9 Abs. 1 Satz 1 Nr. 1 IZG-SH ebenso die öffentliche Sicherheit (Funktionsfähigkeit der „Prüfstelle“) gestört werden könnte (vgl. VG Gelsenkirchen, Urteil vom 28.04.2016, 17 K 4135/15). Das Prüfungsamt erklärte uns, dass es nur eine endliche Aufgabenzahl gebe. Für uns war nachvollziehbar, dass bei Bekanntgabe aller Aufgaben dieses zu einem lediglich punktuellen, auf die Fragen eingeschränkten Lernen führen könne.

Auch die Interessenabwägung, die bei Eingreifen von Ablehnungsgründen durchzuführen war, führte aus unserer Sicht zu keinem anderen Ergebnis. Liegen Ablehnungsgründe vor, ist zu prüfen, ob a) ein öffentliches Bekanntgabeinteresse vorhanden ist und b) wie dieses im Verhältnis zu dem Geheimhaltungsinteresse zu gewichten ist. Unter Berücksichtigung der Intention des Gesetzgebers, mithilfe des IZG-SH die Transparenz, Nachvollziehbarkeit und Akzeptanz behördlichen Handelns zu fördern bzw. die demokratischen Beteiligungsrechte zu stärken (Schleswig-Holsteinischer Landtag, Drs. 14/2374, Seite 11), ist in diesem Fall unserer Einschätzung nach bereits ein öffentliches Bekanntgabeinteresse in Bezug auf die erbetenen Informationen zu verneinen. Vielmehr ist das Interesse der Allgemeinheit unserer Auffassung nach darauf gerichtet, das **ordnungsgemäße, fair ausgerichtete Funktionieren des Prüfungsablaufs sichergestellt** zu wissen.

Auch wenn für uns die Aussage des Prüfungsamts bezüglich der endlichen Aufgabenzahl nachvollziehbar ist, steht es dem Petenten offen, den ablehnenden Bescheid des Prüfungsamts auf dem Rechtsweg zu überprüfen. Auch könnte eine persönliche Anfrage nach Artikel 15 DSGVO zu gespeicherten personenbezogenen Daten gegebenenfalls anders bewertet werden als eine Anfrage nach dem IZG-SH.

12.6 Aufnahme des Begriffs des Betriebs- und Geschäftsgeheimnisses ins IZG-SH

Weiterhin in der Diskussion war der Begriff des Betriebs- und Geschäftsgeheimnisses nach § 10 Nr. 3 IZG-SH (siehe 38. TB, Tz. 12.1). Eine Definition des Begriffs findet sich nicht im IZG-SH, sodass bei der Beurteilung auf entsprechende Rechtsprechung dazu zurückgegriffen wird (vgl. Urteil des VG Schleswig vom 25.03.2015, 8 A 8/14). Jedoch beinhaltet seit April 2019 das Bundesgesetz zum Schutz von Geschäftsgeheimnissen **(GeschGehG) eine entsprechende Definition, die jedoch strenger ist als die oben genannte Rechtsprechung**. So kommt nach § 2 Nr. 1 Buchst. b GeschGehG das Tatbestandsmerkmal der angemessenen Schutzmaßnahme hinzu, das der Geheimnisträger nachweisen muss. Andererseits ist das GeschGehG nicht auf den Bereich der Informationsfreiheit ausgelegt, sondern für den zivilrechtlichen Bereich gedacht.

Einige andere Bundesländer lehnen eine automatische Heranziehung der Definition im GeschGehG ab, auch weil sie teilweise eigene Definitionen im Gesetz haben. Zur Klarstellung ist es unseres Erachtens notwendig, dass eine entsprechende Definition in das IZG-SH aufgenommen wird.

Was ist zu tun?

Das IZG-SH sollte eine Definition für Betriebs- und Geschäftsgeheimnisse erhalten, um Klarheit zu den Voraussetzungen zu schaffen.

12.7 Transparenz und der Pottkieker-Gesetzentwurf

Die Landesregierung hat Ende 2019 den Entwurf eines Gesetzes über die Pflicht zur Offenlegung transparenter Kontrollergebnisse (POTKG) vorgelegt. Dieses in Kurzform „Pottkieker“ genannte Gesetzesvorhaben zielt darauf ab, mehr **Transparenz bei den Ergebnissen der lebensmittelrechtlichen Kontrollen** zu erreichen.

In Ermangelung eines bundesweit einheitlichen Systems werden immer wieder Vorschläge zu „Hygieneampeln“ mit Farben oder Smileys diskutiert, die auch in anderen Ländern wie z. B. Dänemark etabliert sind: Damit können sich Verbraucherinnen und Verbraucher auf einen Blick einen groben Überblick verschaffen, wie gut es um die Hygiene in dem Betrieb bestellt ist. Der Pottkieker-Gesetzentwurf geht einen anderen Weg, indem ein Recht für die Besucherinnen und Besucher eines Restaurants eingeführt werden soll, sich den letzten Kontrollbericht der Lebensmittelüberwachung zeigen zu lassen – auf Papier, direkt vor Ort.

In der Anhörung haben wir betont, dass nach dem Pottkieker-Gesetzentwurf die schon bestehenden Transparenzmöglichkeiten nach dem Verbraucherinformationsgesetz (VIG) und dem IZG-SH unberührt blieben. Ansprüche nach VIG oder IZG-SH könnten also weiterhin wahrgenommen werden. Das POTKG würde **eine zusätzliche Möglichkeit für Transparenz** schaffen.

Eine derartige neue eingeführte Offenbarungspflicht könnte sich sogar positiv auf die Ansprüche nach dem IZG-SH auswirken: Einerseits würde damit die Intention des Gesetzgebers, mit dem Pottkieker-Gesetzentwurf mehr Transparenz in der Lebensmittelüberwachung zu erreichen, auch im Rahmen einer nach §§ 9, 10 IZG-SH durchzuführenden Interessenabwägung zukünftig Berücksichtigung finden müssen. Andererseits soll nach dem Pottkieker-Gesetzentwurf ohnehin eine Fassung des Kontrollberichts vorliegen, bei dem etwaige personenbezogene Daten bereits geschwärzt wurden, sodass kein zusätzlicher Bearbeitungsschritt vor der Zugangsgewährung zu den angefragten Informationen notwendig wäre.

Wir haben in der Anhörung außerdem darauf hingewiesen, dass **Kollisionen mit einem barrierefreien Zugang zu vermeiden** sind. Die geplanten Rege-

lungen gehen von einer visuellen Wahrnehmung mit persönlicher Anwesenheit der Verbraucherin oder des Verbrauchers vor Ort aus. Hierbei müsste vermieden werden, Menschen mit Behinderungen zu diskriminieren, die etwa in ihrer Bewegungsmöglichkeit, in ihrem Sehvermögen oder in der Lesefähigkeit eingeschränkt sind.

Unsere Stellungnahme ist unter diesem Link abrufbar:

http://www.landtag.ltsh.de/infothek/wahl19/umdrucke/03400/umdruck-19-03417.pdf

Kurzlink: *https://uldsh.de/tb39-12-7*

13

KERNPUNKTE

DATENSCHUTZAKADEMIE Schleswig-Holstein

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Die DATENSCHUTZAKADEMIE Schleswig-Holstein ist für die Konzeption und Organisation der Fortbildungsveranstaltungen zu den Themenbereichen Datenschutz und Informationsfreiheit zuständig. Im Einklang mit der Datenschutz-Grundverordnung (DSGVO) wird so beispielsweise den behördlichen und betrieblichen Datenschutzbeauftragten entsprechendes Fachwissen vermittelt.

Nach den beiden sehr **erfolgreichen Schulungsjahren 2018 und 2019**, in denen aufgrund der Einführung der DSGVO eine hohe Nachfrage bestand, war das Jahr 2020 durch Corona und den damit einhergehenden Einschränkungen durch die Maßnahmen zur Bekämpfung der Ausbreitung des Coronavirus geprägt. Im **Schulungsjahr 2020** konnte die DATENSCHUTZAKADEMIE nur eine **geringe Anzahl an Fortbildungsveranstaltungen** anbieten.

Wie auch in den vorangegangenen Jahren wurde ein Teil der Fortbildungsveranstaltungen als Sonderkurse mit speziell auf den Auftraggeber zugeschnittenen Themen im Bereich Datenschutz und Datensicherheit durchgeführt.

Die Schülerkurse „Entscheide DU – sonst tun es andere für dich!“ erfreuten sich im Berichtszeitraum weiterhin großer Beliebtheit. Die Veranstaltungen sind für das Thema **„Datenschutz- und Medienkompetenz“**, besonders mit Fokus auf den Umgang mit ihren eigenen Daten im Internet und in sozialen Medien, konzipiert. Es konnte jedoch in diesem Bereich nur eine sehr geringe Anzahl von Veranstaltungen durchgeführt werden.

Die alljährlich an einem Montag im Spätsommer stattfindende **Sommerakademie** der DATENSCHUTZAKADEMIE fand erstmals seit dem Bestehen des Unabhängigen Landeszentrums für Datenschutz aufgrund der Coronapandemie **nicht statt**. In den vergangenen Jahren zog die Konferenz jeweils knapp 500 Datenschutzexpertinnen und -experten und Interessierte aus dem gesamten Bundesgebiet und darüber hinaus nach Kiel. Unsere Veranstaltung lebt von dem Zusammentreffen der Datenschutz-Community in Präsenz, und die Hygienekonzepte hätten hier nur wenige Teilnehmende zugelassen.

Zu den Themen der letzten Jahre gehörten u. a. **„Verbraucher im Fokus – Herausforderungen und Lösungen des Verbraucherdatenschutzes“** oder **„Update nötig: Beschäftigtendatenschutz im digitalen Zeitalter 4.0“**. Die Präsentationen der Vortragenden aus den letzten Jahren stehen weiterhin auf unserer Webseite zur Verfügung:

https://www.datenschutzzentrum.de/sommerakademie/

Kurzlink: *https://uldsh.de/tb39-13*

Die Vorbereitungen konzentrieren sich jetzt auf das Veranstaltungsjahr 2021.

Index

H

I

J

K

L

M

N

O

P

S

T

V

W

Y

Z

ULD

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein

Schleswig-Holsteins
Zentrum für Datenschutz
und Informationszugang

https://www.datenschutzzentrum.de/tb/